UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
WACO DIVISION

CORRECT TRANSMISSION, LLC Plaintiff, v. JUNIPER NETWORKS, INC. Defendant.	§ § § § § § § § §	 Case No. 20-cv-0670 **JURY TRIAL DEMANDED**

<u>COMPLAINT FOR PATENT INFRINGEMENT</u>

Correct Transmission, LLC ("Correct Transmission" or "Plaintiff"), by and through its attorneys, for its Complaint for patent infringement against Juniper Networks, Inc. ("Juniper" or "Defendant"), and demanding trial by jury, hereby alleges, on information and belief with regard to the actions of Defendant and on knowledge with regard to its own actions, as follows:

I. NATURE OF THE ACTION

1. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 271, *et seq*., to enjoin and obtain damages resulting from Defendant's unauthorized use, sale, and offer to sell in the United States, of products, methods, processes, services and/or systems that infringe Plaintiff's United States patents, as described herein.

2. Defendant manufactures, provides, uses, sells, offers for sale, imports, and/or distributes infringing products and services, and encourages others to use its products and services in an infringing manner, as set forth herein.

3. Plaintiff seeks past and future damages and prejudgment and post-judgment interest for Defendant's infringement of the Asserted Patents, as defined below.

II. PARTIES

4. Plaintiff Correct Transmission is a limited liability company organized and existing under the law of the State of Delaware, with its principal place of business located at 16192 Coastal Highway, Lewes, DE 19958.

5. Correct Transmission is the owner of the entire right, title, and interest of the Asserted Patents, as defined below.

6. Juniper Networks, Inc. ("Juniper"), is a Delaware corporation with its principal place of business at 1133 Innovation Way, Sunnyvale, California 94089. Juniper may be served through its registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. On information and belief, Juniper is registered to do business in the State of Texas and has been since at least April 27, 2017.

7. Juniper conducts business operations within the Western District of Texas in its facilities at 1120 South Capital of Texas Highway, Suite 120, First Floor, Building 2, Austin, Texas 78746. Juniper has offices in the Western District of Texas where it sells and/or markets its products, including an office in Austin, Texas.

III. JURISDICTION AND VENUE

8. This is an action for patent infringement which arises under the patent laws of the United States, in particular, 35 U.S.C. §§ 271, 281, 283, 284, and 285.

9. This Court has exclusive jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

10. This Court has personal jurisdiction over Juniper in this action because Juniper has committed acts within the Western District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Juniper would not offend traditional notions of fair play and substantial justice. Defendant Juniper, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Juniper is registered to do business in the State of Texas, has offices and facilities in the State of Texas, and actively directs its activities to customers located in the State of Texas.

11. Venue is proper in this district under 28 U.S.C. §§ 1391(b)–(d) and 1400(b). Defendant Juniper is registered to do business in the State of Texas, has offices in the State of Texas, and upon information and belief, has transacted business in the Western District of Texas and has committed acts of direct and indirect infringement in the Western District of Texas. Juniper maintains a regular and established place of business in the Western District of Texas, including an office located at 1120 South Capital of Texas Highway, Suite 120, First Floor, Building 2, Austin, Texas 78746.

IV. COUNTS OF PATENT INFRINGEMENT

12. Plaintiff alleges that Defendant has infringed and continue to infringe the following United States patents (collectively the "Asserted Patents"):

United States Patent No. 6,876,669 (the "'669 Patent") (Exhibit A)
United States Patent No. 7,127,523 (the "'523 Patent") (Exhibit B)
United States Patent No. 7,283,465 (the "'465 Patent") (Exhibit C)
United States Patent No. 7,768,928 (the "'928 Patent") (Exhibit D)
United States Patent No. 7,983,150 (the "'150 Patent") (Exhibit E)

COUNT ONE
<u>INFRINGEMENT OF U.S. PATENT 6,876,669</u>

13. Plaintiff incorporates by reference the allegations in all preceding paragraphs as if fully set forth herein.

14. The '669 Patent, entitled "PACKET FRAGMENTATION WITH NESTED INTERRUPTIONS," was filed on January 8, 2001 and issued on April 5, 2005.

15. Plaintiff is the assignee and owner of all rights, title and interest to the '669 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

<u>Technical Description</u>

16. The '669 Patent addresses problems in the prior art of fragmentation, including that a prior art data transmission method "cannot stop until the entire packet has been sent" "once the transmitter has begun sending fragments of a given packet." (col. 3, ll. 6–10). "Thus, the only way that a high-priority packet can be

assured immediate transmission is by discarding any low-priority packets whose transmission is in progress.” (col. 3, ll. 10–13).

17. The ’669 Patent provides a technical solution to prior art problems by applying a “multi-priority approach,” which “allows the transmitter to stop sending the low-priority packet in the middle, and then to complete the transmission after high-priority requirements have been serviced.” Indeed, in a preferred embodiment, any number of increasingly high-priority packets may interrupt transmission of earlier commenced transmissions of lower-priority packets, using “nested” packet interruptions, “without compromising the ability of the receiver to reassemble all of the packets.” (col. 3, ll. 14-30).

Direct Infringement

18. Defendant, without authorization or license from Plaintiff, has been and is directly infringing the ’669 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), importing, selling and offering for sale telecommunications equipment that infringes one or more claims of the ’669 Patent. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringes one or more claims of the ’669 Patent. Defendant further provides services that practice methods that infringe one or more claims of the ’669 Patent. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Juniper MX Series Routers, and all other substantially similar products (collectively the “’669 Accused Products”).

19. Correct Transmission names this exemplary infringing instrumentality to serve as notice of Defendant's infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of '669 Accused Products.

20. Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the manufacture, sale, offer for sale, importation, or distribution of Defendant's MX Series Routers.

21. Juniper's MX Series Routers is a non-limiting example of a router that meets all limitations of claim 15 of the '669 Patent, either literally or equivalently.

22. The Juniper MX Series Router is configured for transmitting data over a channel.


MX SERIES 5G UNIVERSAL ROUTING PLATFORMS

Product Overview

Unrelenting traffic growth—driven by higher speeds, more subscribers, mobile penetration, cloud adoption, and ubiquitous video consumption—is straining traditional service provider and enterprise networks.

Product Description

The continuous expansion of mobile, video, and cloud-based services is disrupting traditional networks and impacting the businesses that rely on them. While annual double-digit traffic growth requires massive resource investments to prevent congestion and accommodate unpredictable traffic spikes, capturing return on that investment can be elusive. Emerging trends such as 5G mobility, Internet of Things (IoT) communications, and the continued growth of cloud networking promise even greater network challenges in the near future. The Juniper Networks® MX Series 5G Universal Routing Platform delivers the industry's first end-to-end infrastructure security solution for enterprises as they look to move business-critical applications to public clouds. Delivering features, functionality, and secure services at scale in the 5G era with no compromises, the MX Series is a critical part of the network evolution happening now.

At the same time, traditional operations environments are increasingly challenged to meet

https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000597-en.pdf

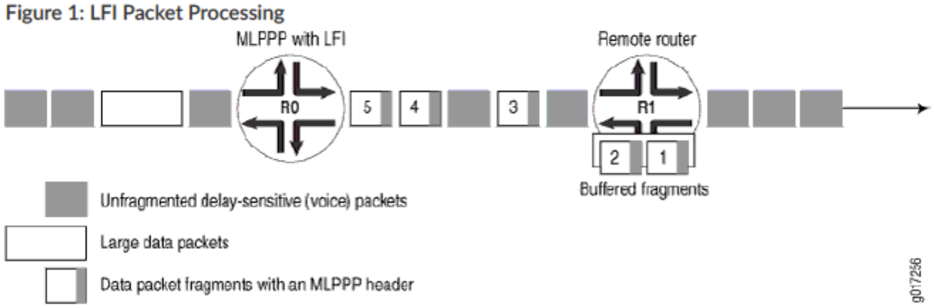
23. The Juniper MX Series Router receives a first datagram for transmission at a first priority.

Priority scheduling on a multilink (MLPPP) bundle determines the order in which an output interface transmits traffic from an output queue. The queues are serviced in a weighted round-robin fashion. But when a queue containing large packets starts using the MLPPP bundle, small and delay-sensitive packets must wait their turn for transmission. Because of this delay, some slow links can become useless for delay-sensitive traffic.

Link fragmentation and interleaving (LFI) solves this problem by reducing delay and jitter on links by fragmenting large packets and interleaving delay-sensitive packets with the resulting smaller packets for simultaneous transmission across multiple links of a MLPPP bundle.

Figure 1 shows how LFI processes packets.

Figure 1: LFI Packet Processing



https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-link-fragmentation-interweaving-understanding.html

Device R0 and Device R1 have LFI enabled. When Device R0 receives large and small packets, such as data and voice packets, it divides them into two categories:

- All voice packets and any other packets configured to be treated as voice packets are categorized as LFI packets and transmitted without fragmentation or an MLPPP header.
- The remaining non-LFI (data) packets are fragmented or unfragmented based on the configured fragmentation threshold. Packets larger than the fragmentation threshold are fragmented. An MLPPP header (containing a multilink sequence number) is added to all non-LFI packets, fragmented and unfragmented.

https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-link-fragmentation-interweaving-understanding.html

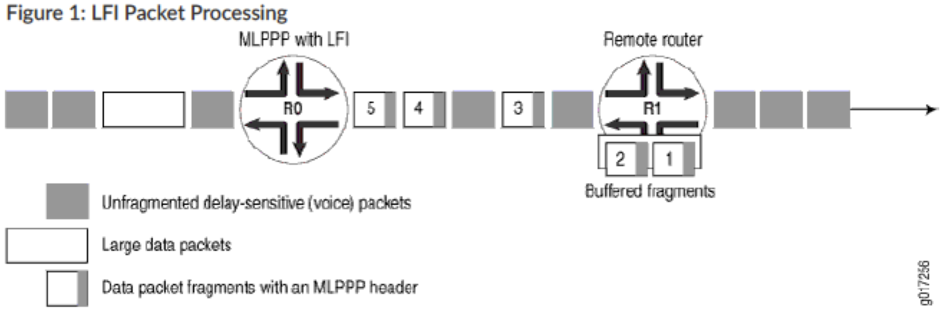
24. The Juniper MX Series Router is configured to receive a second datagram for transmission at a second priority, higher than the first priority, before the transmission of the first datagram is completed.

Priority scheduling on a multilink (MLPPP) bundle determines the order in which an output interface transmits traffic from an output queue. The queues are serviced in a weighted round-robin fashion. But when a queue containing large packets starts using the MLPPP bundle, small and delay-sensitive packets must wait their turn for transmission. Because of this delay, some slow links can become useless for delay-sensitive traffic.

Link fragmentation and interleaving (LFI) solves this problem by reducing delay and jitter on links by fragmenting large packets and interleaving delay-sensitive packets with the resulting smaller packets for simultaneous transmission across multiple links of a MLPPP bundle.

Figure 1 shows how LFI processes packets.

Figure 1: LFI Packet Processing



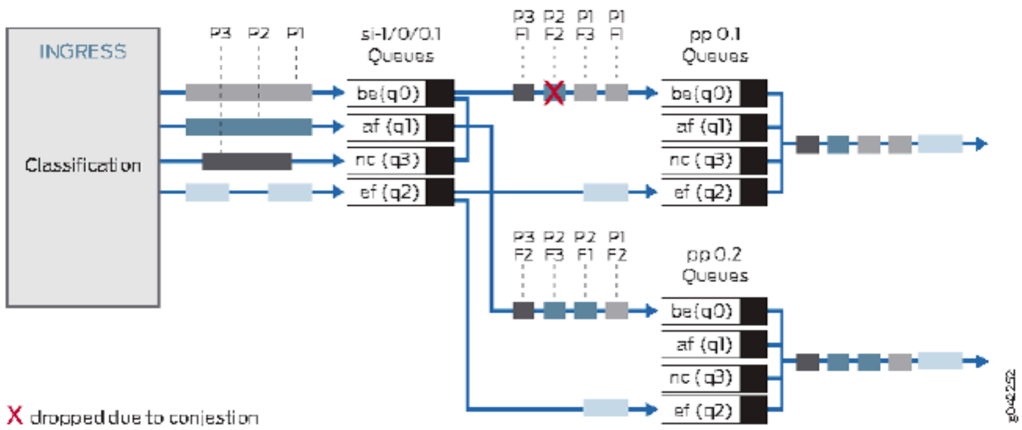
https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-link-fragmentation-interweaving-understanding.html

25. The Juniper MX Series Router is configured to, responsive to receiving the second datagram, decide to divide the first datagram into a plurality of fragments, including a first fragment and a last fragment.

During the first stage of queuing at the `si` interface, when exiting from these queues, LFI packets are fragmented and assigned a sequence number. These fragmented packets are then distributed to the member links where they are queued for the second time.

Congestion at the member link queues can result in MLPPP packet fragments being dropped, as shown in Figure 1. Packet flows in the figure use the notation Px,Fx; for example, P1,F1 represents Packet 1, Fragment 1.

Figure 1: Dropped Sequenced Packet Fragment



https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-sequenced-packet-fragment-drops-understanding.html

Multilink PPP (MLPPP) link fragmentation and interleaving (LFI) provides buffering at the receiver side of a link to reassemble MLPPP fragmented packets. Dropping of the packet fragments is a concern because the packet fragments' remainder consumes valuable bandwidth and buffer space, only to have it eventually being dropped.

The MX Series provides two stages of queuing for packets exiting an MLPPP bundle:

- The first stage of queuing is performed at the inline services `si` interface.
- The second stage is performed by adding member link scheduler queues.

During the first stage of queuing at the `si` interface, when exiting from these queues, LFI packets are fragmented and assigned a sequence number. These fragmented packets are then distributed to the member links where they are queued for the second time.

Congestion at the member link queues can result in MLPPP packet fragments being dropped, as shown in Figure 1. Packet flows in the figure use the notation Px,Fx; for example, P1,F1 represents Packet 1, Fragment 1.

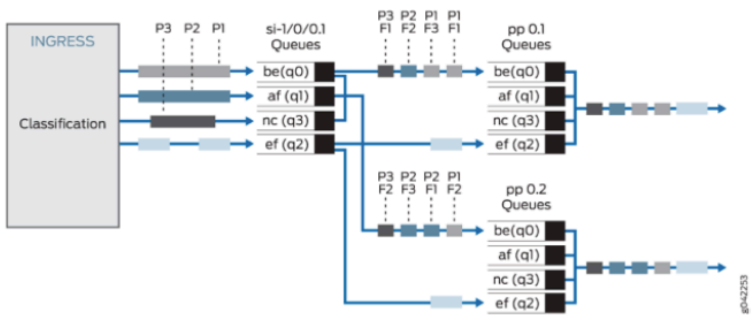
https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-sequenced-packet-fragment-drops-understanding.html

26. The Juniper MX Series Router is configured to transmit the fragments of the first datagram over the channel, beginning with the first fragment.

Figure 1 shows how traffic is queued on an MLPPP multilink bundle and its member links. Packet flows in the figure use the notation Px,Fx; for example, P1,F1 represents Packet 1, Fragment 1.

- There are four queues.
- Forwarding classes be, af, and nc are mapped to queues q0, q1, and q3, respectively, on the multilink bundle. These are fragmented.
- Forwarding class ef contains voice traffic, and is mapped to q2 and is not fragmented.
- Interface `si-1/0/0.1` is the bundle, and `pp0.1` and `pp0.2` are the member links for that bundle.

Figure 1: Queuing on Member Links



https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-sequenced-packet-fragment-drops-understanding.html

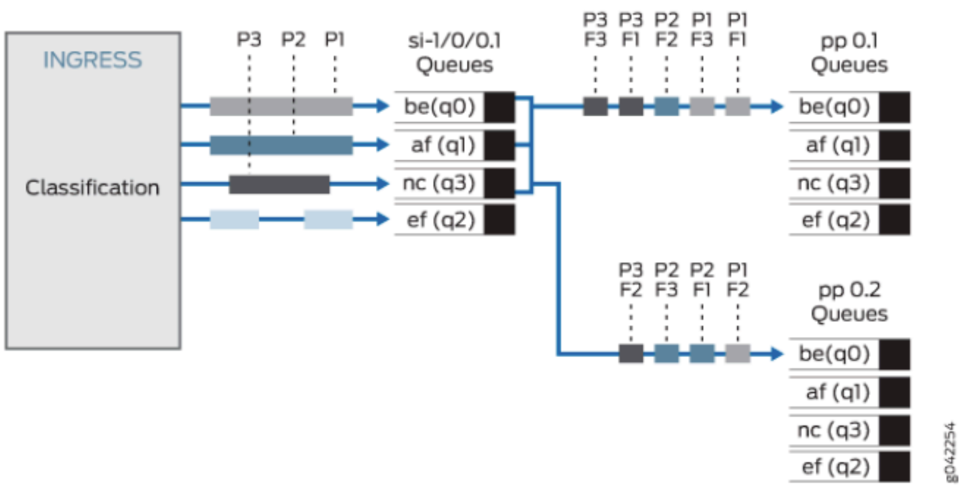
27. The Juniper MX Series Router is configured to transmit at least a fragment of the second datagram over the channel before transmitting the last fragment of the first datagram.

Queuing of Fragmented Packets to Member Links

On a multilink bundle, packet fragments from all forwarding classes with fragmentation enabled are transmitted to q0 on member links. On the q0 queues of member links, packets are queued using a round-robin method to enable per-fragment load balancing.

Figure 2 shows how fragmented packet queuing is performed on the member links. Packet flows in the figure use the notation Px,Fx; for example, P1,F1 represents Packet 1, Fragment 1.

Figure 2: Queuing of Fragmented Packets on Member Links



https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-fragmented-packet-queuing-understanding.html

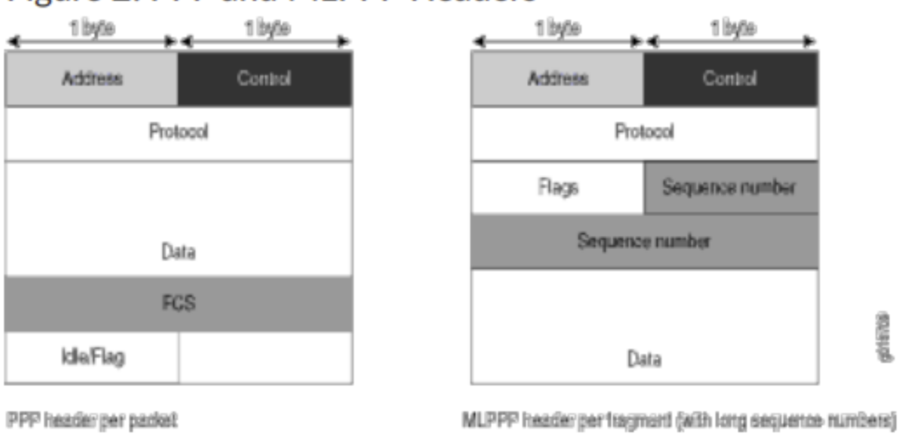
28. The Juniper MX Series Router is configured wherein transmitting at least the fragment of the second datagram comprises interrupting transmission of a number of datagrams, including at least the first datagram, in order to transmit at least the fragment of the second datagram, and adding a field to the fragment indicating the number of datagrams whose transmission has been interrupted.

Fragmented Multilink PPP (MLPPP) packets have a multilink header containing a multilink sequence number. The sequence numbers on these fragments must be preserved so that the remote device receiving these fragments can correctly reassemble them into a complete packet. To accommodate this requirement, Junos OS queues all packets on member links of a multilink bundle with a MLPPP header into a single queue (q0) by default.

- Traffic flows of a forwarding class that has MLPPP fragmentation configured are distributed from the inline services `si` bundle interface queues to the member link queues (queue 0) following a round-robin method.
- Traffic flows of a forwarding class without MLPPP fragmentation are distributed from the `si` bundle interface queues to the member link queues based on a hashing algorithm computed from the destination address, source address, and IP protocol of the packet.
  If the IP payload contains TCP or UDP traffic, the hashing algorithm also includes the source and destination ports. As a result, all traffic belonging to one traffic flow is queued to one member link.

https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-fragmented-packet-queuing-understanding.html

Figure 2: PPP and MLPPP Headers



https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-interface-config-link-service-interface.html

Willful Infringement

29. Defendant has had actual knowledge of the ’669 Patent and its infringement thereof at least as of receipt of Plaintiff’s notice letter dated May 9, 2017.

30. Defendant has had actual knowledge of the ’669 Patent and its infringement thereof at least as of service of Plaintiff’s Complaint.

31. Defendant’s infringement of the patents-in-suit was either known or was so obvious that it should have been known to Defendant.

32. Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard willfully infringed the ’669 Patent. Defendant continued to commit acts of infringement despite being on notice of an objectively high likelihood that its actions constituted infringement of Plaintiff’s valid patent rights, either literally or equivalently.

33. This objective risk was either known or so obvious that it should have been known to Defendant. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

34. Defendant has induced and is knowingly inducing its distributors, testers, trainers, customers and/or end users to directly infringe the ’669 Patent, with the specific intent to induce acts constituting infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

35. Defendant has knowingly contributed to direct infringement by its customers and end users by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the accused products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

36. Defendant's indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support that induce its customers and/or end users to directly infringe '669 Patent, including: Understanding Fragmented Packet Queuing - TechLibrary - Juniper Networks; Understanding MLPPP and Fragmentation-Maps - TechLibrary - Juniper Networks; Understanding MLPPP Link Fragmentation and Interleaving - TechLibrary - Juniper Networks; and Understanding MLPPP Link Fragmentation and Interleaving - TechLibrary - Juniper Networks.

37. Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's indirect infringement further includes providing application notes instructing its customers on infringing uses of the '669 Accused Products. The '669 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the '669 Patent, either literally or equivalently. Defendant knows and intends that customers who purchase the '669 Accused Products will use those

products for their intended purpose. For example, Defendant's United States website: https://www.juniper.net, instructs customers to use the '669 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional videos on YouTube (https://www.youtube.com/user/JuniperNetworks/videos), its website, and elsewhere providing instructions on using the '669 Accused Products. Defendant's customers directly infringe the '669 Patent when they follow Defendant's provided instructions on its website, videos, and elsewhere. Defendant's customers who follow Defendant's provided instructions directly infringe claims of the '669 Patent.

38. In addition, Defendant specifically intends that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendant's infringing products. Defendant knows following its instructions directly infringes claims of the '669 Patent, including for example Claim 1.

39. Juniper MX Series routers implement a method for transmitting data over a channel.

MX SERIES 5G UNIVERSAL ROUTING PLATFORMS

Product Overview

Unrelenting traffic growth—driven by higher speeds, more subscribers, mobile penetration, cloud adoption, and ubiquitous video consumption—is straining traditional service provider and enterprise networks.

Product Description

The continuous expansion of mobile, video, and cloud-based services is disrupting traditional networks and impacting the businesses that rely on them. While annual double-digit traffic growth requires massive resource investments to prevent congestion and accommodate unpredictable traffic spikes, capturing return on that investment can be elusive. Emerging trends such as 5G mobility, Internet of Things (IoT) communications, and the continued growth of cloud networking promise even greater network challenges in the near future. The Juniper Networks® MX Series 5G Universal Routing Platform delivers the industry's first end-to-end infrastructure security solution for enterprises as they look to move business-critical applications to public clouds. Delivering features, functionality, and secure services at scale in the 5G era with no compromises, the MX Series is a critical part of the network evolution happening now.

At the same time, traditional operations environments are increasingly challenged to meet

https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000597-en.pdf

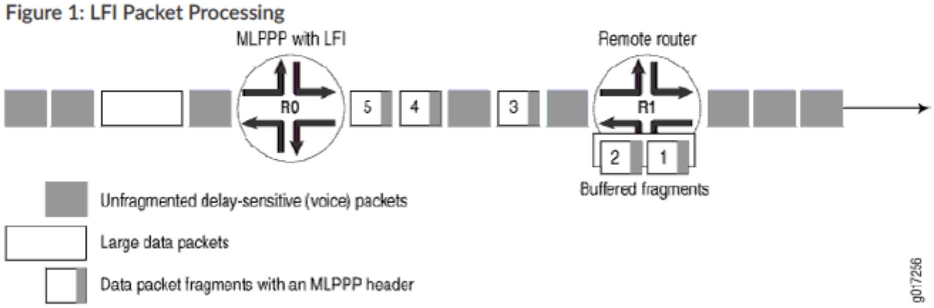
40. Juniper MX Series routers receive a first datagram for transmission at a first priority.

Priority scheduling on a multilink (MLPPP) bundle determines the order in which an output interface transmits traffic from an output queue. The queues are serviced in a weighted round-robin fashion. But when a queue containing large packets starts using the MLPPP bundle, small and delay-sensitive packets must wait their turn for transmission. Because of this delay, some slow links can become useless for delay-sensitive traffic.

Link fragmentation and interleaving (LFI) solves this problem by reducing delay and jitter on links by fragmenting large packets and interleaving delay-sensitive packets with the resulting smaller packets for simultaneous transmission across multiple links of a MLPPP bundle.

Figure 1 shows how LFI processes packets.

Figure 1: LFI Packet Processing



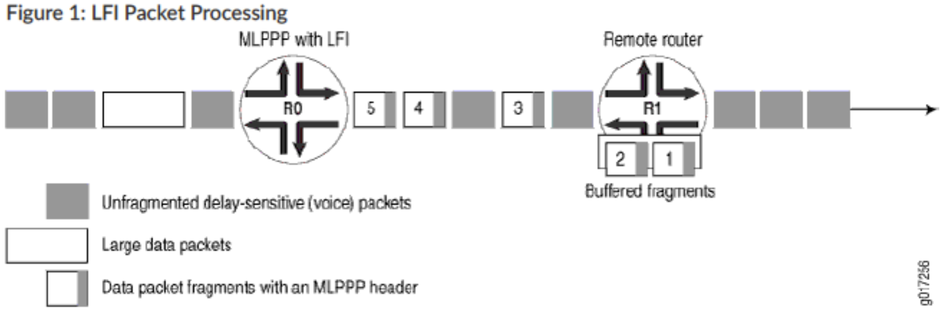
https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-link-fragmentation-interweaving-understanding.html

> Device R0 and Device R1 have LFI enabled. When Device R0 receives large and small packets, such as data and voice packets, it divides them into two categories:
>
> - All voice packets and any other packets configured to be treated as voice packets are categorized as LFI packets and transmitted without fragmentation or an MLPPP header.
> - The remaining non-LFI (data) packets are fragmented or unfragmented based on the configured fragmentation threshold. Packets larger than the fragmentation threshold are fragmented. An MLPPP header (containing a multilink sequence number) is added to all non-LFI packets, fragmented and unfragmented.

https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-link-fragmentation-interweaving-understanding.html

41. Juniper MX Series routers receive a second datagram for transmission at a second priority, higher than the first priority, before the transmission of the first datagram is completed.

> Priority scheduling on a multilink (MLPPP) bundle determines the order in which an output interface transmits traffic from an output queue. The queues are serviced in a weighted round-robin fashion. But when a queue containing large packets starts using the MLPPP bundle, small and delay-sensitive packets must wait their turn for transmission. Because of this delay, some slow links can become useless for delay-sensitive traffic.
>
> Link fragmentation and interleaving (LFI) solves this problem by reducing delay and jitter on links by fragmenting large packets and interleaving delay-sensitive packets with the resulting smaller packets for simultaneous transmission across multiple links of a MLPPP bundle.
>
> Figure 1 shows how LFI processes packets.
>
> Figure 1: LFI Packet Processing



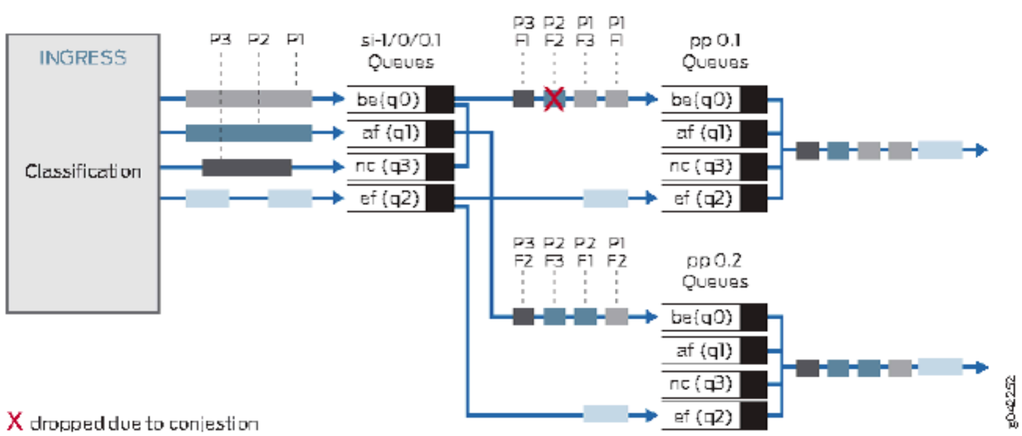
https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-link-fragmentation-interweaving-understanding.html

42. Juniper MX Series routers, responsive to receiving the second datagram, decide to divide the first datagram into a plurality of fragments, including a first fragment and a last fragment.

During the first stage of queuing at the `si` interface, when exiting from these queues, LFI packets are fragmented and assigned a sequence number. These fragmented packets are then distributed to the member links where they are queued for the second time.

Congestion at the member link queues can result in MLPPP packet fragments being dropped, as shown in Figure 1. Packet flows in the figure use the notation Px,Fx; for example, P1,F1 represents Packet 1, Fragment 1.

Figure 1: Dropped Sequenced Packet Fragment



https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-sequenced-packet-fragment-drops-understanding.html

> Multilink PPP (MLPPP) link fragmentation and interleaving (LFI) provides buffering at the receiver side of a link to reassemble MLPPP fragmented packets. Dropping of the packet fragments is a concern because the packet fragments' remainder consumes valuable bandwidth and buffer space, only to have it eventually being dropped.
>
> The MX Series provides two stages of queuing for packets exiting an MLPPP bundle:
>
> - The first stage of queuing is performed at the inline services `si` interface.
> - The second stage is performed by adding member link scheduler queues.
>
> During the first stage of queuing at the `si` interface, when exiting from these queues, LFI packets are fragmented and assigned a sequence number. These fragmented packets are then distributed to the member links where they are queued for the second time.
>
> Congestion at the member link queues can result in MLPPP packet fragments being dropped, as shown in Figure 1. Packet flows in the figure use the notation Px,Fx; for example, P1,F1 represents Packet 1, Fragment 1.

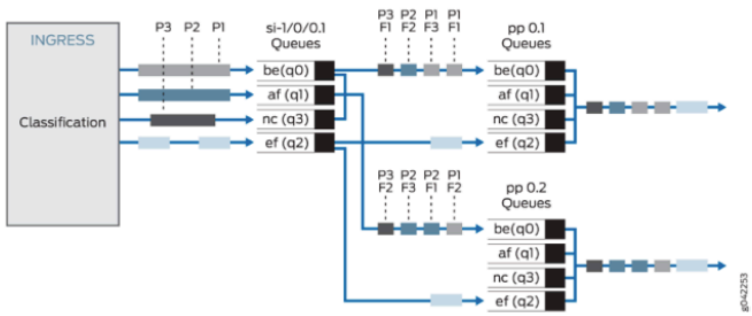
https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-sequenced-packet-fragment-drops-understanding.html

43. Juniper MX Series routers transmit the fragments of the first datagram over the channel, beginning with the first fragment.

Figure 1 shows how traffic is queued on an MLPPP multilink bundle and its member links. Packet flows in the figure use the notation Px,Fx; for example, P1,F1 represents Packet 1, Fragment 1.

- There are four queues.
- Forwarding classes be, af, and nc are mapped to queues q0, q1, and q3, respectively, on the multilink bundle. These are fragmented.
- Forwarding class ef contains voice traffic, and is mapped to q2 and is not fragmented.
- Interface `si-1/0/0.1` is the bundle, and `pp0.1` and `pp0.2` are the member links for that bundle.

Figure 1: Queuing on Member Links



https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-sequenced-packet-fragment-drops-understanding.html

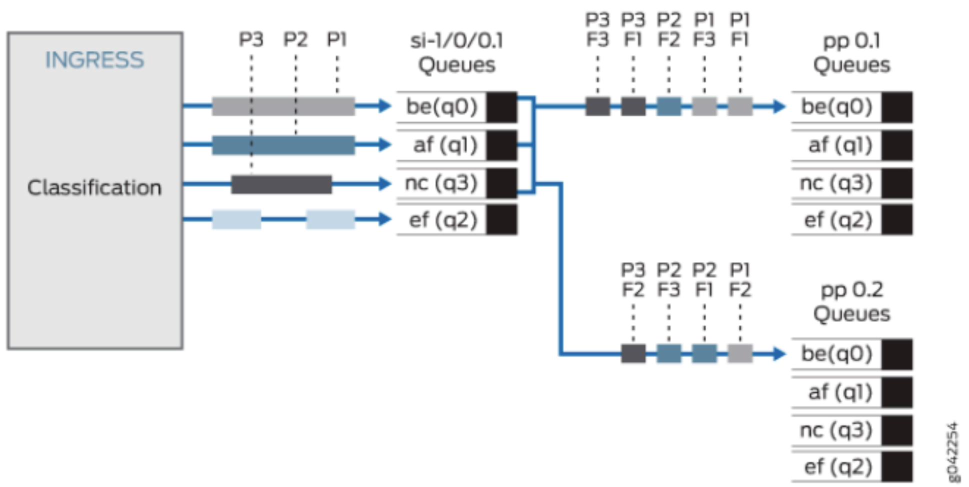
44. Juniper MX Series routers transmit at least a fragment of the second datagram over the channel before transmitting the last fragment of the first datagram.

Queuing of Fragmented Packets to Member Links

On a multilink bundle, packet fragments from all forwarding classes with fragmentation enabled are transmitted to q0 on member links. On the q0 queues of member links, packets are queued using a round-robin method to enable per-fragment load balancing.

Figure 2 shows how fragmented packet queuing is performed on the member links. Packet flows in the figure use the notation Px,Fx; for example, P1,F1 represents Packet 1, Fragment 1.

Figure 2: Queuing of Fragmented Packets on Member Links



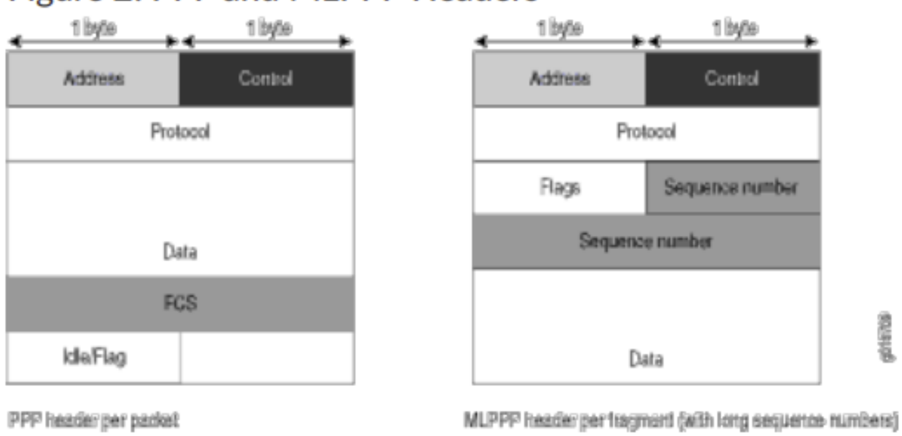
https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-fragmented-packet-queuing-understanding.html

45. In Juniper MX Series routers, transmitting at least the fragment of the second datagram comprises interrupting transmission of a number of datagrams, including at least the first datagram, in order to transmit at least the fragment of the second datagram, and adding a field to the fragment indicating the number of datagrams whose transmission has been interrupted.

> Fragmented Multilink PPP (MLPPP) packets have a multilink header containing a multilink sequence number. The sequence numbers on these fragments must be preserved so that the remote device receiving these fragments can correctly reassemble them into a complete packet. To accommodate this requirement, Junos OS queues all packets on member links of a multilink bundle with a MLPPP header into a single queue (q0) by default.
>
> - Traffic flows of a forwarding class that has MLPPP fragmentation configured are distributed from the inline services `si` bundle interface queues to the member link queues (queue 0) following a round-robin method.
> - Traffic flows of a forwarding class without MLPPP fragmentation are distributed from the `si` bundle interface queues to the member link queues based on a hashing algorithm computed from the destination address, source address, and IP protocol of the packet.
>   If the IP payload contains TCP or UDP traffic, the hashing algorithm also includes the source and destination ports. As a result, all traffic belonging to one traffic flow is queued to one member link.

https://www.juniper.net/documentation/en_US/junos/topics/concept/mlppp-fragmented-packet-queuing-understanding.html

Figure 2: PPP and MLPPP Headers



https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-interface-config-link-service-interface.html

46. As a result of Defendant's infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such

infringement which, by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT TWO
INFRINGEMENT OF U.S. PATENT 7,127,523

47. Plaintiff incorporates by reference the allegations in preceding paragraphs 1-12 as if fully set forth herein.

48. The ’523 Patent, entitled “SPANNING TREE PROTOCOL TRAFFIC IN A TRANSPARENT LAN” was filed on January 25, 2002 and issued on October 24, 2006.

49. Plaintiff is the assignee and owner of all rights, title and interest to the ’523 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

Technical Description

50. The ’523 Patent addresses problems in the prior art of local-area-network (LAN) technology, including prior-art attempts to prevent problematic data-packet-communication loops in transparent LAN services (TLS). Prior attempts were “costly and difficult to maintain,” had “security and reliability drawbacks,” were “excessively complex to configure,” and/or were largely theoretical, failing to account for issues stemming from the “separation of provider and user domains.” (col. 4, l. 61 – col. 5, l. 15)

51. The ’523 Patent provides a solution to the prior art problems by disclosing improved equipment and an improved method “for preventing loops in a

TLS network." (col. 5, ll. 63-64) In preferred embodiments, "STP [spanning tree protocol] frames are sent through the same tunnels as the user traffic, but are distinguished from the user data frames by a special STP label. Loop removal is carried out in this way for each one of the TLSs, so that each TLS has its own loop-free topology. Using this method, the TLS network operator is able to ensure that there are no loops in the core network, irrespective of loops that users may add when they connect their own equipment to the network." (col. 6, ll. 2-9).

Direct Infringement

52. Defendant, without authorization or license from Plaintiff, has been and is directly infringing the '523 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), importing, selling and offering for sale methods, devices, and networks infringing one or more claims of the '523 Patent. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringes one or more claims of the '523 Patent. Defendant further provides services that practice methods that infringe one or more claims of the '523 Patent. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Juniper Networks' EX2300 Multigigabit Ethernet Switches, and all other substantially similar products (collectively the "'523 Accused Products").

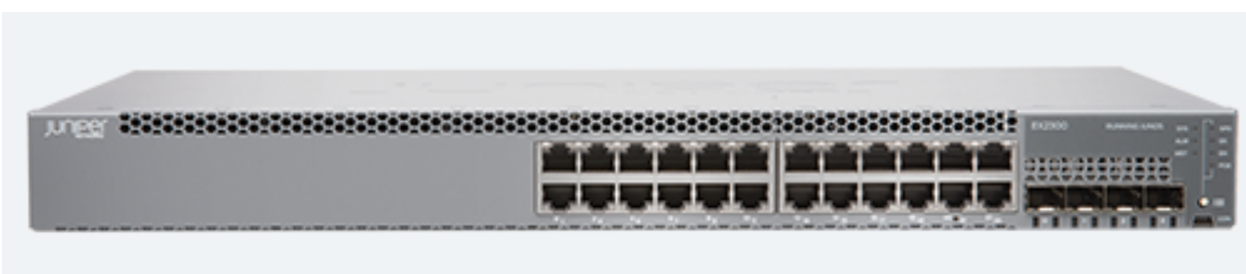
53. Correct Transmission names these exemplary infringing instrumentalities to serve as notice of Defendant's infringing acts, but Correct

Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of ’523 Accused Products.

54. Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, importation, or distribution of Defendant’s EX2300 Multigigabit Ethernet Switches.

55. Defendant’s EX2300 Multigigabit Ethernet Switches is a non-limiting example of an ethernet switch that meets all limitations of claim 10 of the ’523 Patent, either literally or equivalently.

56. Defendant’s EX2300 Multigigabit Ethernet Switches comprise a communication device for operation as one of a plurality of label-switched routers (LSRs) in a transparent local area network service (TLS), which includes a system of label-switched tunnels between the label-switched routers (LSRs) through a communication network, the TLS having at least first and second endpoints to which first and second user equipment is connected so that the TLS acts as a virtual bridge between the first and second user equipment.



EX2300

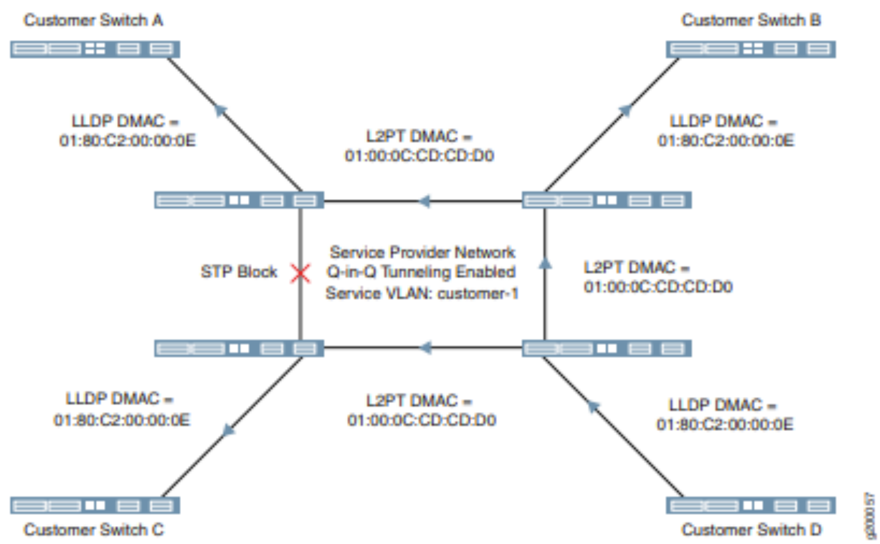
The EX2300 Ethernet Switch delivers a compact, high-density, cost-effective solution for small network environments where space and power are at a premium.

https://www.juniper.net/us/en/products-services/switching/ex-series/

Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain. This feature is useful when you want to run Layer 2 protocols on a network that includes switches located at remote sites that are connected across a service provider network.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

Figure 10: L2PT Example



https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

57. Defendant's EX2300 Multigigabit Ethernet Switches comprises one or more ports, adapted to send and receive traffic via the label-switched tunnels.

EX2300 Multigigabit Ethernet Switch

Overview

The EX2300 Multigigabit Ethernet Switch delivers a compact 1 U high-density solution for small network environments with space, power, and budget constraints. The 802.11ac Wave 2 access points connect to the EX2300 Multigigabit switches, thereby providing investment protection by using existing cabling infrastructure to support multigigabit speeds and higher throughput demands. The EX2300 Multigigabit switches are perfect for refreshing network access infrastructures or building new greenfield campus and branch deployments that require multigigabit ports on the access switch.

There are two EX2300 Multigigabit switch models available, offering either 24 or 48 10/100 Mbps/1GbE/2.5GbE-T ports in a single platform. Both models offer IEEE 802.3af Power over Ethernet (PoE)/802.3at PoE+ for powering attached network devices. Each switch has 10GbE small form-factor pluggable plus transceiver (SPF+ transceiver) uplink ports that support connections to other access or distribution layer switches.

EX2300 Multigigabit switches integrate with Juniper's industry-leading Virtual Chassis technology to simplify operations by consolidating the management of up to four switches into one logical device. These switches can also form a Virtual Chassis with existing non-multigigabit EX2300 switches. Additionally, EX2300 Multigigabit switches are supported as satellite devices in a Junos Fusion Enterprise deployment, which allows large numbers of access switches to be merged into a logical management platform.

https://www.juniper.net/us/en/products-services/switching/ex-series/ex2300m/

58. Defendant's EX2300 Multigigabit Ethernet Switches comprises a traffic processor which is coupled to the one or more ports, and is adapted to transmit control frames to the LSRs in the TLS via the label-switched tunnels, each control frame comprising a control traffic label and a bridge protocol data unit (BPDU) in accordance with a spanning tree protocol (STP), the control traffic label indicating to the LSRs that the STP is to be executed by the LSRs without transmission of the BPDU to the user equipment, wherein the traffic processor is further adapted, upon

receiving the control frames, to process the BPDU, responsively to the control traffic label, so as to remove loops in a topology of the TLS irrespective of the user equipment.

> ## Understanding BPDU Protection for Spanning-Tree Instance Interfaces
>
> MX Series routers, ACX Series routers, and EX Series switches support spanning-tree protocols that prevent loops in a network by creating a tree topology (spanning-tree) of the entire bridged network. All spanning-tree protocols use a special type of frame called bridge protocol data units (BPDUs) to communicate with each other. Other devices in the network, such as PCs, generate their own BPDUs that are not compatible with the spanning-tree BPDUs. When BPDUs generated by other devices are transmitted to switches on which spanning-tree protocols are configured, a misconfiguration can occur in the spanning tree and a network outage can occur. Therefore, it is necessary to protect an interface in a spanning-tree topology from BPDUs generated from other devices.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/spanning-tree-bpdu-protection.html#id-example-configuring-bpdu-protection-on-edge-interfaces-to-prevent-stp-miscalculations-on-non-els-ex-series-switches

Willful Infringement

59. Defendant has had actual knowledge of the '523 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated May 9, 2017.

60. Defendant has had actual knowledge of the '523 Patent and its infringement thereof at least as of service of Plaintiff's Complaint.

61. Defendant's risk of infringement of the patents-in-suit was either known or was so obvious that it should have been known to Defendant.

62. Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard willfully infringed the '523 Patent. Defendant has thus had actual

notice of the infringement of the ’523 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff’s valid patent rights, either literally or equivalently.

63. This objective risk was either known or so obvious that it should have been known to Defendant. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

64. Defendant has induced and is knowingly inducing its customers and/or end users to directly infringe the ’523 Patent, with the specific intent to encourage such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

65. Defendant has knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the ’523 Accused Products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

66. Defendant’s indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support that induce its customers and/or end users to directly infringe ’523 Patent, including the EX2300 Multigigabit Ethernet Switch Overview and Ethernet Switching Feature Guide for EX Series Switches.

67. Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's indirect infringement further includes providing application notes instructing its customers on infringing uses of the accused products. The '523 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the '523 Patent, either literally or equivalently. Defendant knows and intends that customers who purchase the '523 Accused Products will use those products for their intended purpose. For example, Defendant's United States website: https://www.juniper.net, instructs customers to use the '523 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional videos on YouTube (https://www.youtube.com/user/JuniperNetworks/videos), its website, and elsewhere providing instructions on using the '523 Accused Products. Defendant's customers directly infringe the '523 Patent when they follow Defendant's provided instructions on its website, videos, and elsewhere. Defendant's customers who follow Defendant's provided instructions directly infringe claims of the '523 Patent.

68. In addition, Defendant specifically intends that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendant's infringing products. Defendant knows following its instructions directly infringes claims of the '523 Patent, including for example Claim 1.

69. Defendant’s customers who follow Defendant’s provided instructions directly infringe the method of Claim 1 of the ’523 Patent.

70. Defendant instructs its customers to use its EX2300 Multigigabit Ethernet Switches in a method for communication.

EX2300

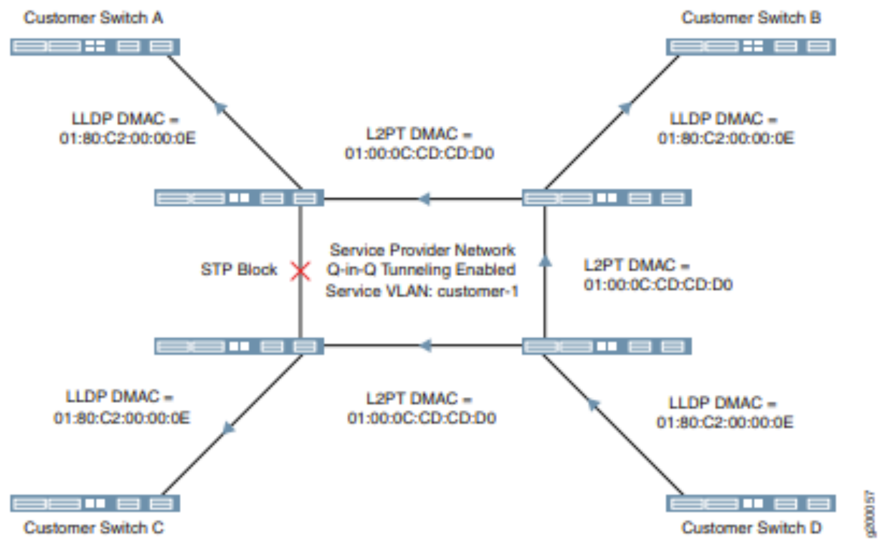
The EX2300 Ethernet Switch delivers a compact, high-density, cost-effective solution for small network environments where space and power are at a premium.

https://www.juniper.net/us/en/products-services/switching/ex-series/

> Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider’s cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain. This feature is useful when you want to run Layer 2 protocols on a network that includes switches located at remote sites that are connected across a service provider network.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

Figure 10: L2PT Example



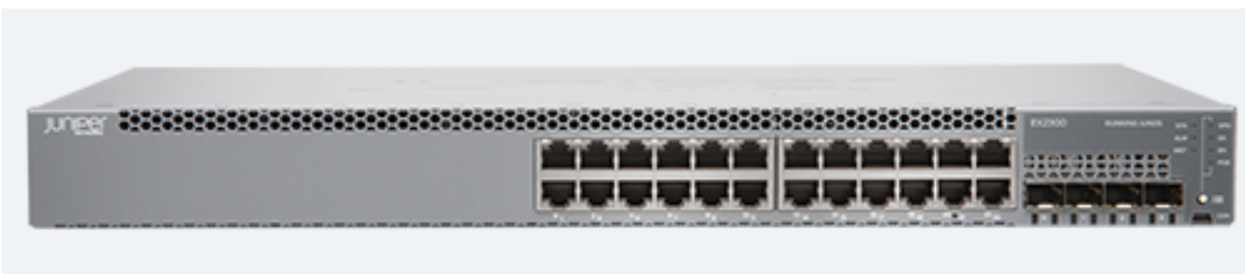
https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

71. Defendant instructs its customers to use its EX2300 Multigigabit Ethernet Switches to define a topology of a transparent local area network service (TLS), comprising a system of label-switched tunnels between label-switched routers (LSRs) through a communication network, the TLS having at least first and second endpoints to which first and second user equipment is connected so that the TLS acts as a virtual bridge between the first and second user equipment.

Understanding BPDU Protection for Spanning-Tree Instance Interfaces

MX Series routers, ACX Series routers, and EX Series switches support spanning-tree protocols that prevent loops in a network by creating a tree topology (spanning-tree) of the entire bridged network. All spanning-tree protocols use a special type of frame called bridge protocol data units (BPDUs) to communicate with each other. Other devices in the network, such as PCs, generate their own BPDUs that are not compatible with the spanning-tree BPDUs. When BPDUs generated by other devices are transmitted to switches on which spanning-tree protocols are configured, a misconfiguration can occur in the spanning tree and a network outage can occur. Therefore, it is necessary to protect an interface in a spanning-tree topology from BPDUs generated from other devices.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/spanning-tree-bpdu-protection.html#id-example-configuring-bpdu-protection-on-edge-interfaces-to-prevent-stp-miscalculations-on-non-els-ex-series-switches



EX2300

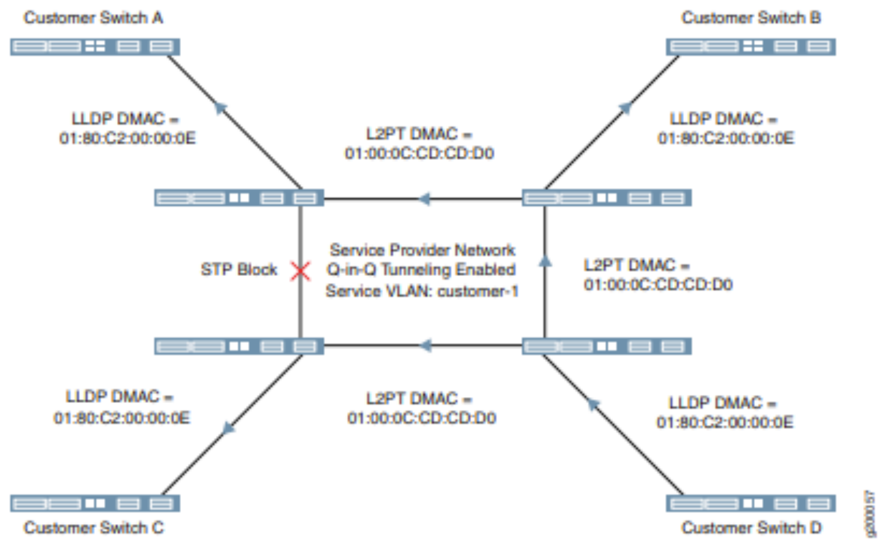
The EX2300 Ethernet Switch delivers a compact, high-density, cost-effective solution for small network environments where space and power are at a premium.

https://www.juniper.net/us/en/products-services/switching/ex-series/

Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain. This feature is useful when you want to run Layer 2 protocols on a network that includes switches located at remote sites that are connected across a service provider network.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

Figure 10: L2PT Example



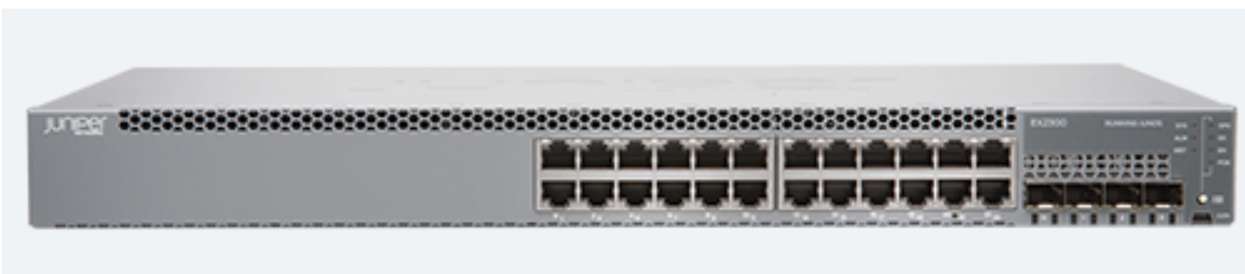
https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

72. Defendant instructs its customers to use its EX2300 Multigigabit Ethernet Switches to transmit control frames among the LSRs in the TLS via the label-switched tunnels, each control frame comprising a control traffic label and a bridge protocol data unit (BPDU) in accordance with a spanning tree protocol (STP), the control traffic label indicating to the LSRs that the STP is to be executed by the LSRs without transmission of the BPDU to the user equipment.

Understanding BPDU Protection for Spanning-Tree Instance Interfaces

MX Series routers, ACX Series routers, and EX Series switches support spanning-tree protocols that prevent loops in a network by creating a tree topology (spanning-tree) of the entire bridged network. All spanning-tree protocols use a special type of frame called bridge protocol data units (BPDUs) to communicate with each other. Other devices in the network, such as PCs, generate their own BPDUs that are not compatible with the spanning-tree BPDUs. When BPDUs generated by other devices are transmitted to switches on which spanning-tree protocols are configured, a misconfiguration can occur in the spanning tree and a network outage can occur. Therefore, it is necessary to protect an interface in a spanning-tree topology from BPDUs generated from other devices.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/spanning-tree-bpdu-protection.html#id-example-configuring-bpdu-protection-on-edge-interfaces-to-prevent-stp-miscalculations-on-non-els-ex-series-switches



EX2300

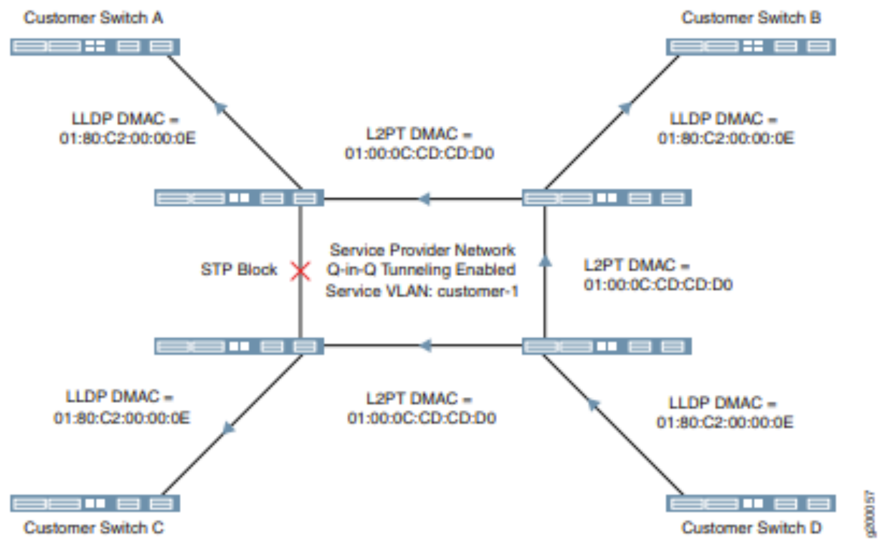
The EX2300 Ethernet Switch delivers a compact, high-density, cost-effective solution for small network environments where space and power are at a premium.

https://www.juniper.net/us/en/products-services/switching/ex-series/

Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain. This feature is useful when you want to run Layer 2 protocols on a network that includes switches located at remote sites that are connected across a service provider network.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

Figure 10: L2PT Example



https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

73. Defendant instructs its customers to use its EX2300 Multigigabit Ethernet Switches, upon receiving the control frames at the LSRs, to process the BPDU, responsively to the control traffic label, so as to remove loops in the topology of the TLS irrespective of the user equipment.

Understanding BPDU Protection for Spanning-Tree Instance Interfaces

MX Series routers, ACX Series routers, and EX Series switches support spanning-tree protocols that prevent loops in a network by creating a tree topology (spanning-tree) of the entire bridged network. All spanning-tree protocols use a special type of frame called bridge protocol data units (BPDUs) to communicate with each other. Other devices in the network, such as PCs, generate their own BPDUs that are not compatible with the spanning-tree BPDUs. When BPDUs generated by other devices are transmitted to switches on which spanning-tree protocols are configured, a misconfiguration can occur in the spanning tree and a network outage can occur. Therefore, it is necessary to protect an interface in a spanning-tree topology from BPDUs generated from other devices.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/spanning-tree-bpdu-protection.html#id-example-configuring-bpdu-protection-on-edge-interfaces-to-prevent-stp-miscalculations-on-non-els-ex-series-switches

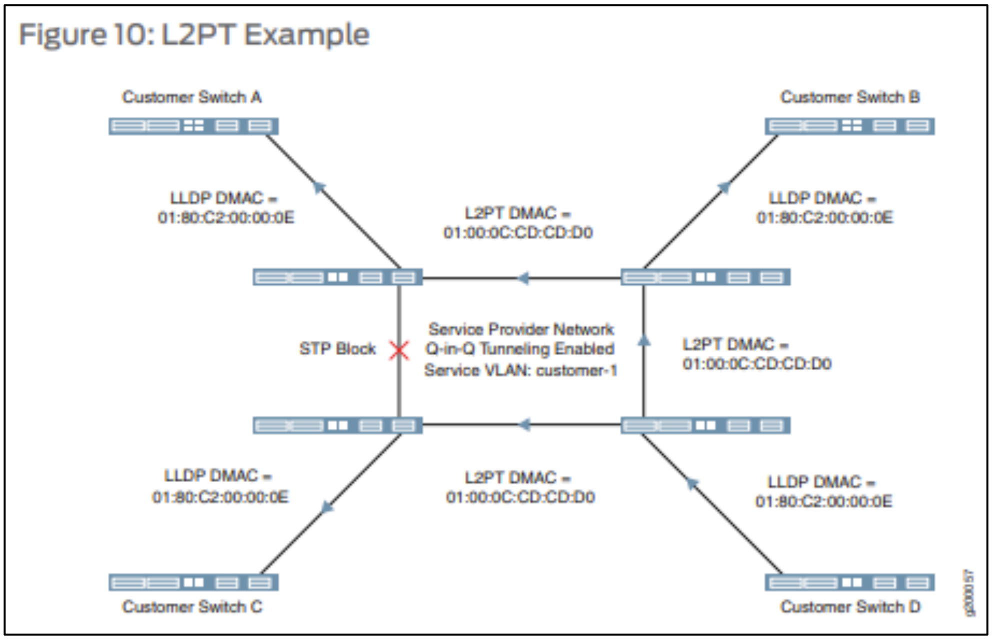
EX2300

The EX2300 Ethernet Switch delivers a compact, high-density, cost-effective solution for small network environments where space and power are at a premium.

https://www.juniper.net/us/en/products-services/switching/ex-series/

> Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain. This feature is useful when you want to run Layer 2 protocols on a network that includes switches located at remote sites that are connected across a service provider network.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf



https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/ex-series/ethernet-switching-vlans-ex-series.pdf

74. As a result of Defendant's infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement which, by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

COUNT THREE
INFRINGEMENT OF U.S. PATENT 7,283,465

75. Plaintiff incorporates by reference the allegations in preceding paragraphs 1-12 as if fully set forth herein.

76. The '465 Patent, entitled "HIERARCHICAL VIRTUAL PRIVATE LAN SERVICE PROTECTION SCHEME" was filed on January 7, 2003 and issued on October 16, 2007.

77. Plaintiff is the assignee and owner of all rights, title and interest to the '465 Patent, including the right to recover for past infringements, and has the legal

right to enforce the patent, sue for infringement, and seek equitable relief and damages.

<u>Technical Description</u>

78. The ’465 Patent addresses technical problems in the prior art of LAN networks that may result from failures in network nodes. Existing failure protection systems may use “backup point-to-point PWs between each edge node and an additional core node. The backup PW connection is in addition to the standard PW connection already existing between the edge node and another code node. Thus, if a VC between an edge node and a core node fails, a backup ‘protection path’ through another core node can be used to provide access between the edge node and the rest of the network.” (col. 4, ll. 18-33). Such systems however suffer from “long period[s] of traffic outage if a virtual connection fails between an edge node and a core node, or if a code node fails. In most cases, initiation of failure protection depends on MAC address aging and learning schemes, which are slow.” *Id*. Further, there are no provisions for handling multiple failures at once and the need to handle both standard connections (to edge nodes and other core nodes) and backup protection connections (to edge nodes) complicates the design of the core nodes and the network as a whole. *Id*.

79. The ’465 Patent “seeks to provide improved mechanisms for protection from failure in virtual private networks (VPNs)” by using a network comprising primary core nodes and standby core nodes having the same topology as a corresponding primary core node which it protects. (col. 4, l. 50-col. 5, l. 39). “[I]f the

primary core node fails, the remaining nodes in the network simply redirect all connections from the failed primary core node to the corresponding standby core node. Since the standby core node has the same topology as the failed primary core node, the remaining nodes in the network do not need to re-learn MAC table addresses, and are thus able to recover quickly from the failure. In addition, there is no need to clear the MAC tables, so that packet flooding is reduced significantly." *Id.*

Direct Infringement

80. Defendant, without authorization or license from Plaintiff, has been and is directly infringing the '465 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), importing, selling and offering for sale methods, devices, and networks infringing one or more claims of the '465 Patent. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringes one or more claims of the '465 Patent. Defendant further provides services that practice methods that infringe one or more claims of the '465 Patent. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Juniper Networks EX9200 Ethernet Switches, and all other substantially similar products (collectively the "'465 Accused Products").

81. Correct Transmission names these exemplary infringing instrumentalities to serve as notice of Defendant's infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or

learned by Correct Transmission or revealed during discovery, and include them in the definition of '465 Accused Products.

82. Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, importation, or distribution of Defendant's EX9200 Ethernet Switches.

83. Defendant's EX9200 Ethernet Switches are non-limiting examples of ethernet switches that meet all limitations of claim 1 of the '465 Patent, either literally or equivalently.

84. Defendant's EX9200 Ethernet Switches are configured to comprise a data communication network.

https://www.juniper.net/us/en/products-services/switching/ex-series/ex9200/

Overview

The EX9200 line of Ethernet switches provides a programmable, flexible, and scalable foundation for delivering mission-critical applications in enterprise campus and data center core environments.

EX9200 switches simplify the deployment of cloud applications, server virtualization, and rich media collaboration tools in enterprise campus and data center core and aggregation environments.

In the enterprise campus, the EX9200 enables collaboration and provides simple and secure access for the delivery of mission-critical applications. In the data center, it simplifies operations to align the network with fast-changing business requirements.

The EX9200 switches also serve as the foundation for the Junos Fusion Enterprise architecture, a new standards-based approach for creating an open, highly scalable switch fabric for the enterprise campus. Junos Fusion Enterprise dramatically simplifies campus deployments by collapsing the entire network into a single management point, with the EX9200 as its core. Junos Fusion Enterprise can also serve as the shared core for enterprise campus environments that have on-premise data centers.

Three EX9200 switches are available: the EX9204, EX9208, and EX9214. The EX9200 chassis deliver up to 240 Gbps (full duplex) per slot. A pass-through midplane design supports capacity of up to 13.2 Tbps for built-in migration to next-generation deployments. Any combination of 1GbE, 10GbE, and 40GbE interfaces can be used, and the switches include support for 100GbE cards when available.

https://www.juniper.net/us/en/products-services/switching/ex-series/ex9200/

Use Case for Configuring MC-LAG on the Core for Campus Networks

The core is the heart of the campus network, and in today's mission critical enterprise environments, the flow of business requires that the network is always available. Increasing traffic loads and link resiliency are key considerations for campus network builders. The multichassis LAG (MC-LAG) feature set on the Juniper Networks EX9200 family of switches is an ideal solution for providing options for optimizing link utilization and ensuring high availability in the campus core.

MC-LAG in a campus configuration allows you to bond two or more physical links into a logical link between core-aggregation or aggregation-access switches. MC-LAG improves availability by providing active/active links between multiple switches over a standard link aggregation group (LAG), eliminates the need for the Spanning Tree Protocol (STP), and provides faster Layer 2 convergence upon link and device failures. With multiple active network paths, MC-LAG enables you to load-balance traffic across the multiple physical links. If a link fails, the traffic can be forwarded through the other available links and the aggregated link remains available.

A common campus deployment model for MC-LAG with the EX9200 positions the EX9200 at the campus core using a collapsed core and aggregation model where access layer switches are logically grouped into a Virtual Chassis and uplink directly to the EX9200. In this collapsed model, the EX9200 is providing Layer 2 and Layer 3 services to the downstream network. With this scenario, MC-LAG is used between the core switches to provide a resilient, high bandwidth path to the downstream access layer. With the EX9200 providing routing at the campus core, MC-LAG is configured to support multiple VLANS with associated IRB interfaces, presented to the access network as a standard LAG group.

This configuration gives operators the benefits of increased bandwidth and link efficiency between the campus core and access layers, link resiliency between layers, along with the survivability provided by independent control and management planes.

https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-145-mc-lag-ex-core-campus.pdf

85. Defendant's EX9200 Ethernet Switches are configured to comprise a plurality of primary virtual bridges, interconnected by primary virtual connections so as to transmit and receive data packets over the network to and from edge devices connected thereto.

Figure 5: Topology Diagram

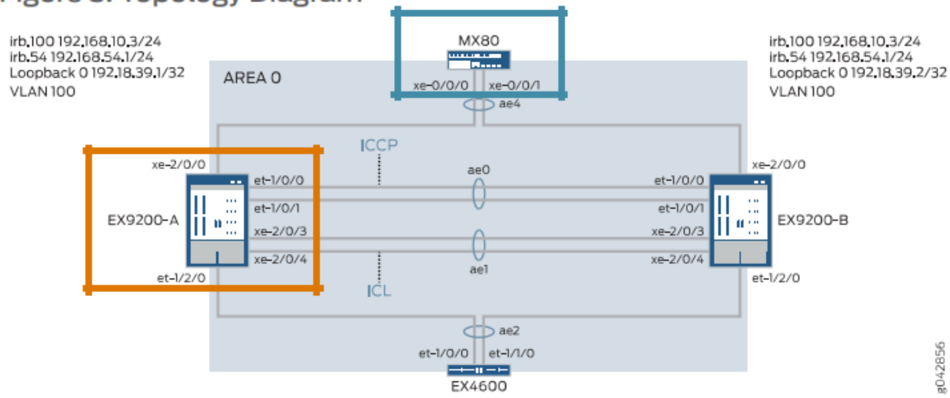


Table 3 on page 30 details the topology used in this configuration example.

Table 3: Components of the Topology for Configuring a Multichassis LAG Between Two Switches

Hostname	Base Hardware	Multichassis Link Aggregation Group
EX9200-A	EX9200	ae0 is configured as an aggregated Ethernet interface, and is used as an ICCP link. The following interfaces are part of ae0: et-1/0/0 and et-1/0/1 on EX9200-A and et-1/0/0 and et-1/0/1 on EX9200-B. ae1 is configured as an aggregated Ethernet interface and is used as an ICL link, and the following two interfaces are part of ae1: xe-2/0/3 and xe-2/0/4 on EX9200-A and xe-2/0/3 and xe-2/0/4 on EX9200-B. ae2 is configured as an MC-LAG, and the following interfaces are part of ae2: et-1/2/0 on EX9200-A and et-1/2/0 on EX9200-B. ae4 is configured as an MC-LAG, and the following interfaces are part of ae4: xe-2/0/0 on EX9200-A and xe-2/0/0 on EX9200-B.
EX9200-B	EX9200	

https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-145-mc-lag-ex-core-campus.pdf

Topology

The topology used in this section of the configuration is shown in Figure 2.

Figure 2: Interface Configuration Between Edge, Perimeter, and Core

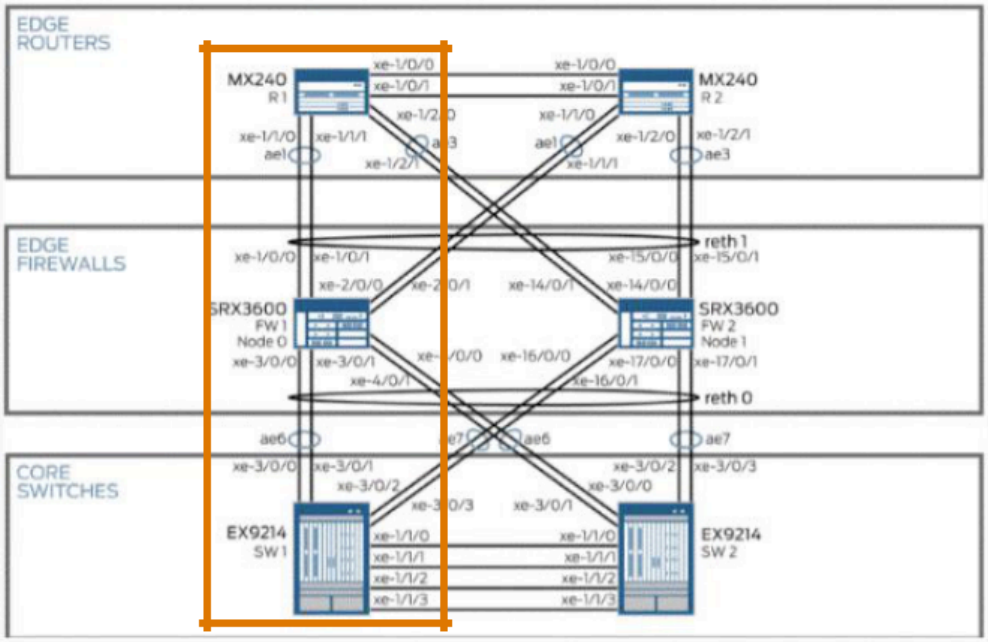


Table 1 shows the configuration parameters used in the configuration of MC-LAG between the VDC-core-sw1 and the edge-r1 nodes. These settings are used throughout the configuration and are aggregated here.

https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/mf-architecture-network-configuration.html

86. Defendant's EX9200 Ethernet Switches are configured to comprise a plurality of backup virtual bridges, each such backup virtual bridge being paired with a corresponding one of the primary virtual bridges and connected by secondary virtual connections to the other primary virtual bridges.

VRRP over IRB

Junos OS supports active/active MC-LAGs by using VRRP in active/standby mode. VRRP in active/standby mode enables Layer 3 routing over the multichassis aggregated Ethernet (MC-AE) interfaces on the MC-LAG peers. In this mode, the MC-LAG peers act as virtual routers. The peers share the virtual IP address that corresponds to the default route configured on the host or server connected to the MC-LAG. This virtual IP address (of the IRB interface) maps to either of the VRRP MAC addresses or to the logical interfaces of the MC-LAG peers. The host or server uses the VRRP MAC address to send any Layer 3 upstream packets.

At any time, one of the VRRP devices is the master (active), and the other is a backup (standby). Usually, a VRRP backup node does not forward incoming packets. However, when VRRP over IRB is configured in an MC-LAG active/active environment, both the VRRP master and the VRRP backup forward Layer 3 traffic arriving on the MC-AE interface, as shown in Figure 4 on page 18. If the master fails, all the traffic shifts to the MC-AE link on the backup.

https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-145-mc-lag-ex-core-campus.pdf

Topology

The topology used in this section of the configuration is shown in Figure 2.

Figure 2: Interface Configuration Between Edge, Perimeter, and Core

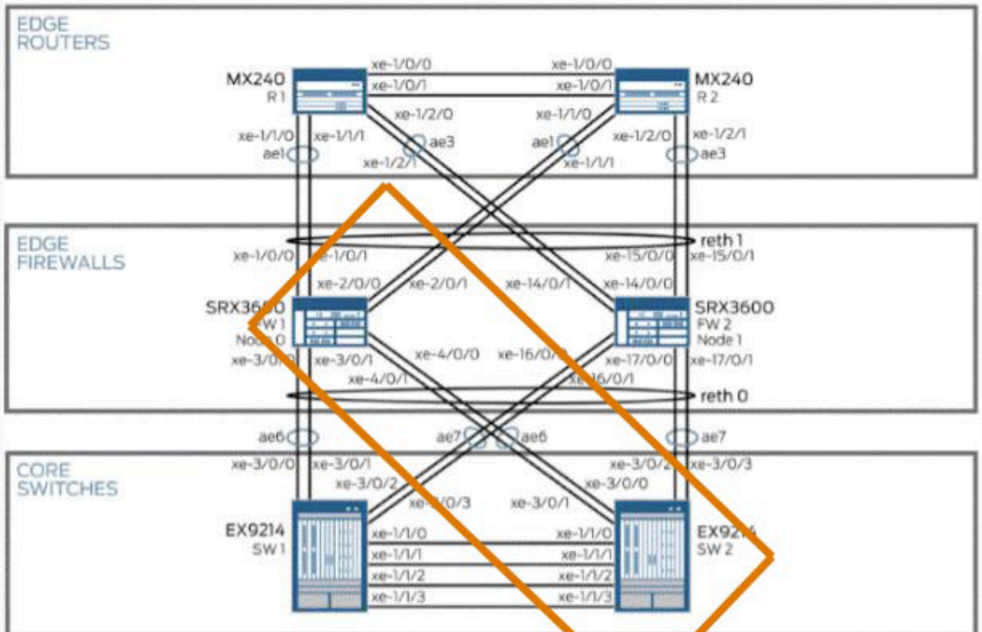


Table 1 shows the configuration parameters used in the configuration of MC-LAG between the VDC-core-sw1 and the edge-r1 nodes. These settings are used throughout the configuration and are aggregated here.

https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/mf-architecture-network-configuration.html

87. Defendant's EX9200 Ethernet Switches are configured wherein the primary virtual connections define a respective primary topology image for each of the primary virtual bridges, and wherein each of the backup virtual bridges is connected to the other primary virtual bridges by secondary virtual connections that are identical to the primary virtual connections of the corresponding one of the primary virtual bridges, thus defining a respective secondary topology image that is identical to the respective primary topology image of the corresponding one of the primary virtual bridges.

Topology

The topology used in this section of the configuration is shown in Figure 2.

Figure 2: Interface Configuration Between Edge, Perimeter, and Core

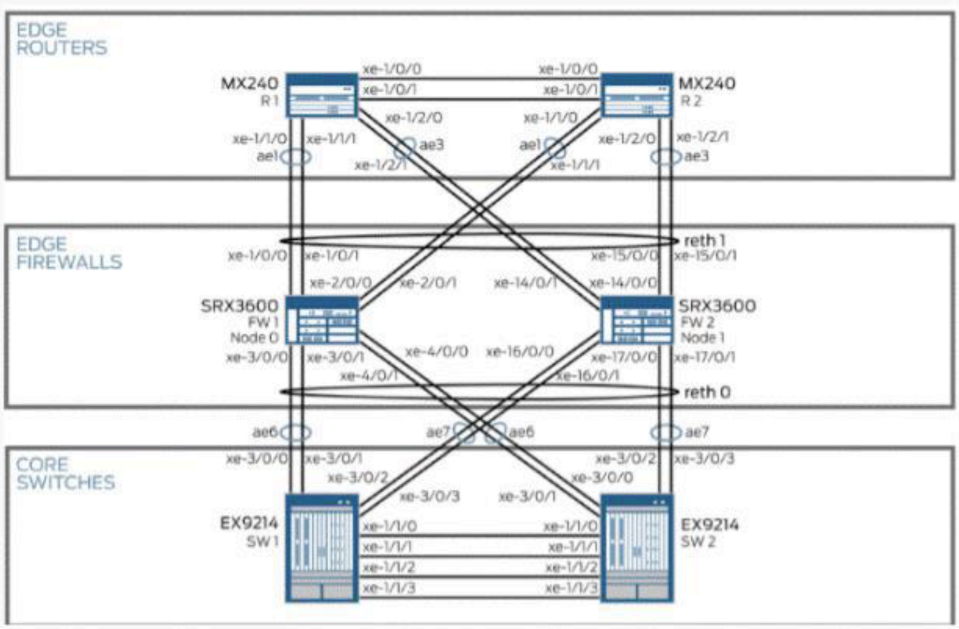


Table 1 shows the configuration parameters used in the configuration of MC-LAG between the VDC-core-sw1 and the edge-r1 nodes. These settings are used throughout the configuration and are aggregated here.

https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/mf-architecture-network-configuration.html

88. Defendant's EX9200 Ethernet Switches are configured wherein each of the primary and backup virtual bridges is adapted to maintain a respective forwarding table, and to forward the data packets in accordance with entries in the respective forwarding table, and wherein each of the backup virtual bridges is adapted to periodically synchronize its forwarding table by copying contents of the forwarding table of the corresponding one of the primary virtual bridges with which it is paired.

MAC Address Management

Without proper MAC address management, an MC-LAG configuration could result in unnecessary flooding. For example:

- When an MC-LAG is configured to be active/active, upstream and downstream traffic could go through different MC-LAG peer devices. This means that the MAC address learned on one peer would have to be relearned on the other peer, causing unnecessary flooding.
- A single-homed client's MAC address is learned only on the MC-LAG peer that it is attached to. If a client attached to the peer MC-LAG network device needs to communicate with that single-homed client, then traffic would be flooded on the peer MC-LAG network device.

To avoid unnecessary flooding, whenever a MAC address is learned on one of the MC-LAG peers, the address is replicated to the other MC-LAG peer. MAC address replication is performed as follows:

- MAC addresses learned on an MC-LAG of one MC-LAG peer are replicated as learned on the same MC-LAG of the other MC-LAG peer.
- MAC addresses learned on single-homed clients of one MC-LAG peer are replicated as learned on the ICL interface of the other MC-LAG peer.
- MAC address learning from the data path is disabled on the ICL. MAC address learning on the ICL depends on software installing MAC addresses replicated through ICCP.

https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-145-mc-lag-ex-core-campus.pdf

MAC Address Synchronization

MAC address synchronization enables an MC-LAG peer to forward Layer 3 packets arriving on MC-AE interfaces with either its own IRB MAC address or its peer's IRB MAC address. Each MC-LAG peer installs its own IRB MAC address as well as the peer's IRB MAC address in the hardware. Each MC-LAG peer treats the packet as if it were its own packet. If MAC address synchronization is not enabled, the IRB MAC address is installed on the MC-LAG peer as if it was learned on the ICL.

https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-145-mc-lag-ex-core-campus.pdf

89. Defendant's EX9200 Ethernet Switches are configured whereby upon a failure of the corresponding one of the primary virtual bridges, each of the backup virtual bridge forwards and receives the data packets over the network via the

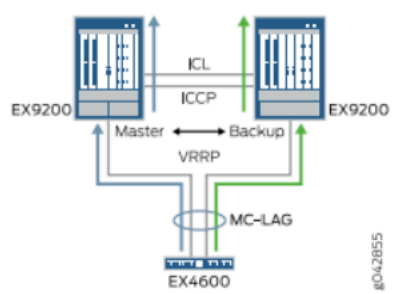
secondary virtual connections, in accordance with the synchronized forwarding table, in place of the corresponding one of the primary virtual bridges.

VRRP over IRB

Junos OS supports active/active MC-LAGs by using VRRP in active/standby mode. VRRP in active/standby mode enables Layer 3 routing over the multichassis aggregated Ethernet (MC-AE) interfaces on the MC-LAG peers. In this mode, the MC-LAG peers act as virtual routers. The peers share the virtual IP address that corresponds to the default route configured on the host or server connected to the MC-LAG. This virtual IP address (of the IRB interface) maps to either of the VRRP MAC addresses or to the logical interfaces of the MC-LAG peers. The host or server uses the VRRP MAC address to send any Layer 3 upstream packets.

At any time, one of the VRRP devices is the master (active), and the other is a backup (standby). Usually, a VRRP backup node does not forward incoming packets. However, when VRRP over IRB is configured in an MC-LAG active/active environment, both the VRRP master and the VRRP backup forward Layer 3 traffic arriving on the MC-AE interface, as shown in Figure 4 on page 18. If the master fails, all the traffic shifts to the MC-AE link on the backup.

Figure 4: VRRP Forwarding in MC-LAG Configuration



MAC Address Synchronization

MAC address synchronization enables an MC-LAG peer to forward Layer 3 packets arriving on MC-AE interfaces with either its own IRB MAC address or its peer's IRB MAC address. Each MC-LAG peer installs its own IRB MAC address as well as the peer's IRB MAC address in the hardware. Each MC-LAG peer treats the packet as if it were its own packet. If MAC address synchronization is not enabled, the IRB MAC address is installed on the MC-LAG peer as if it was learned on the ICL.

https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-145-mc-lag-ex-core-campus.pdf

Willful Infringement

90. Defendant has had actual knowledge of the ’465 Patent and its infringement thereof at least as of receipt of Plaintiff’s notice letter dated May 9, 2017.

91. Defendant has had actual knowledge of the ’465 Patent and its infringement thereof at least as of service of Plaintiff’s Complaint.

92. Defendant’s risk of infringement of the patents-in-suit was either known or was so obvious that it should have been known to Defendant.

93. Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard willfully infringed the ’465 Patent. Defendant has thus had actual notice of the infringement of the ’465 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff’s valid patent rights, either literally or equivalently.

94. This objective risk was either known or so obvious that it should have been known to Defendant. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

95. Defendant has induced and is knowingly inducing its customers and/or end users to directly infringe the ’465 Patent, with the specific intent to encourage

such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

96. Defendant has knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the '465 Accused Products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

97. Defendant's indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support that induce its customers and/or end users to directly infringe '465 Patent, including the EX9200 Ethernet Switch Overview, Configuring MC-LAG on EX9200 Switches in the Core for Campus Networks, and Network Configuration.

98. Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's indirect infringement further includes providing application notes instructing its customers on infringing uses of the accused products. The '465 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the '465 Patent, either literally or equivalently. Defendant knows and intends that customers who purchase the '465 Accused Products will use those products for their intended purpose. For example, Defendant's United States website

https://www.juniper.net, instructs customers to use the ’465 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional videos on YouTube (https://www.youtube.com/user/JuniperNetworks/videos), its website, and elsewhere providing instructions on using the ’465 Accused Products. Defendant’s customers directly infringe the ’465 Patent when they follow Defendant’s provided instructions on its website, videos, and elsewhere. Defendant’s customers who follow Defendant’s provided instructions directly infringe claims of the ’465 Patent.

99. In addition, Defendant specifically intends that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendant’s infringing products.

100. As a result of Defendant’s infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement which, by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

COUNT FOUR
INFRINGEMENT OF U.S. PATENT 7,768,928

101. Plaintiff incorporates by reference the allegations in preceding paragraphs 1-12 as if fully set forth herein.

102. The ’928 Patent, entitled “CONNECTIVITY FAULT MANAGEMENT (CFM) IN NETWORKS WITH LINK AGGREGATION GROUP CONNECTIONS” was filed on July 11, 2006 and issued on August 3, 2010.

103. Plaintiff is the assignee and owner of all rights, title and interest to the '928 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

Technical Description

104. The '928 Patent addresses problems in the prior art of Ethernet service network maintenance, including that prior art CFM systems and techniques "cannot detect certain malfunctions" because "[w]hen a certain network such as a local area network (LAN) or a virtual-LAN (V-LAN) employs LAG interfaces, some of the connectivity fault management functions as currently specified by the IEEE 802.1ag Standard and ITU-T Recommendation Y.1731 cannot be utilized." (col. 2, ll. 31–36). When LAG interfaces are used, packets, which are forwarded from one entity to another, are not sent via a known single fixed network link but via a set of aggregated output links that comprise a single logical port or link. *Id.* The packets are distributed among the links and therefore "the path of each packet cannot be predicted by the originating ME that initiates the CFM function. This could affect the reception of reply messages and performance results such as frame delay variation." *Id.*

105. The '928 Patent provides a solution to the problems in the prior art by providing "a system for implementing fault management functions in networks with LAG connections which are devoid of the above limitations." (col. 3, ll. 1–3). Specifically, the '928 Patent provides a technical solution to the problem by using a

"maintenance entity operable in an Ethernet Connectivity Fault Management (CFM) domain. The maintenance entity comprises a port definer module and a connection configured to be connected to a group of aggregated links. The port definer module is configured to examine a designated link of the group by forwarding at least one CFM message via the designated link." (col. 3, ll. 5–14). "The port definer module is configured for allowing the separate examination of a designated link of the group of LAG members. The examination is done by facilitating the forwarding of CFM messages via the probed designated link." (col. 6, ll. 20–33).

Direct Infringement

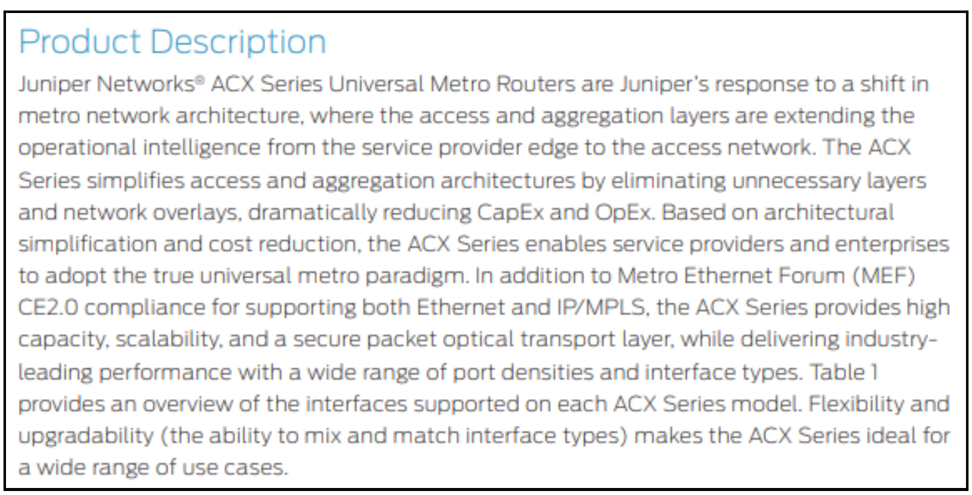
106. Defendant, without authorization or license from Plaintiff, has been and is directly infringing the '928 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), importing, selling and offering for sale methods, devices, and networks infringing one or more claims of the '928 Patent. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringes one or more claims of the '928 Patent. Defendant further provides services that practice methods that infringe one or more claims of the '928 Patent. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Juniper Networks ACX Series Universal Metro Routers (including the ACX500 Router), and all other substantially similar products (collectively the "'928 Accused Products").

107. Correct Transmission names this exemplary infringing instrumentality to serve as notice of Defendant's infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of '928 Accused Products.

108. Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the development, design, manufacture, sale, or distribution of Defendant's ACX Series Universal Metro Routers.

109. Defendant's ACX Series Universal Metro Routers is a non-limiting example of a router that meets all limitations of claim 22 of the '928 Patent, either literally or equivalently.

110. Defendant's ACX Series Universal Metro Routers are configured to execute a method for implementing connectivity fault management (CFM) functions in a network.



Product Description

Juniper Networks® ACX Series Universal Metro Routers are Juniper's response to a shift in metro network architecture, where the access and aggregation layers are extending the operational intelligence from the service provider edge to the access network. The ACX Series simplifies access and aggregation architectures by eliminating unnecessary layers and network overlays, dramatically reducing CapEx and OpEx. Based on architectural simplification and cost reduction, the ACX Series enables service providers and enterprises to adopt the true universal metro paradigm. In addition to Metro Ethernet Forum (MEF) CE2.0 compliance for supporting both Ethernet and IP/MPLS, the ACX Series provides high capacity, scalability, and a secure packet optical transport layer, while delivering industry-leading performance with a wide range of port densities and interface types. Table 1 provides an overview of the interfaces supported on each ACX Series model. Flexibility and upgradability (the ability to mix and match interface types) makes the ACX Series ideal for a wide range of use cases.

https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000397-en.pdf

	Features	ACX500, ACX500-O, ACX500-O-POE	ACX1000, ACX1100	ACX2100, ACX2200	ACX4000	ACX5048, ACX5096
Services	IEEE 802.3 bridge domain	√	√	√	√	√
	PWE (T-LDP)	√	√	√	√	√
	L2VPN (BGP)	√	√	√	√	√
	VPLS (T-LDP/BGP/LDP autodiscovery)					√
	EVPN-ELINE (PWE)					
	EVPN-ELINE (FXC)					
	Layer 3 VPN	√	√	√	√	√
	Circuit emulation SAToP/CESoPSN/ATM o MPLS		√[2]	√[2]	√	
	Integrated routing and bridging (IRB)	√	√	√	√	√
	Stateless filters L2-L4	√	√	√	√	√
Class of Service (CoS)	8 queues per port with schedulers and shaping	√	√	√	√	√
	Classification based on 802.1p, DiffServ code point (DSCP), IP-precedence, Exp bit	√	√	√	√	√
	Single-rate policer ingress/egress	√	√	√	√	√
	Two-rate three-color policer ingress/egress	√	√	√	√	√
	Per-Port Egress Shapping	√	√	√	√	√
	H-QoS					√
OAM and SLA Management	Bidirectional Forwarding Detection (BFD)	√	√	√	√	√
	Connectivity fault management (CFM)	√	√	√	√	√
	Y.1731	√	√	√	√	√[3]
	RFC2544	√	√	√	√	√[4]
	TWAMP	√	√	√	√	

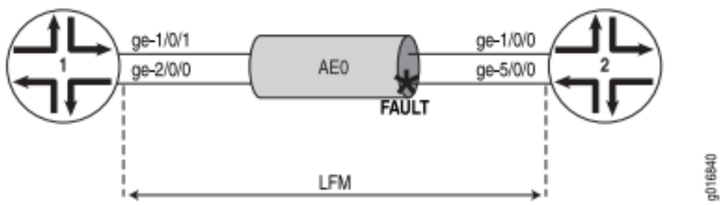
https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000397-en.pdf

111. Defendant's ACX Series Universal Metro Routers are configured to connect first and second maintenance entities via a link aggregation group (LAG), said LAG comprising a single logical link made up of a plurality of physical links

In this example, LFM is configured on an aggregated Ethernet interface (AE0) between Router 1 and Router 2. When configured on aggregated Ethernet, LFM runs on all the individual member links. LFM is enabled or disabled on the member links as they are added or deleted from the aggregation group. The status of individual links is used to determine the status of the aggregated interface.

The use of LFM with aggregated Ethernet is shown in Figure 50 on page 688.

Figure 50: Ethernet LFM for Aggregated Ethernet



https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces-ethernet.pdf

112. Defendant's ACX Series Universal Metro Routers are configured to use said first maintenance entity to select one of said physical links as a designated link for forwarding a CFM message via a designated link of said LAG.

Continuity Check Protocol Parameters Overview

The continuity check protocol is used for fault detection by maintenance end points (MEPs) within a maintenance association. The MEP periodically sends continuity check multicast messages. The continuity check protocol packets use the ethertype value 0x8902 and the multicast destination MAC address 01:80:c2:00:00:32.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces-ethernet.pdf

Understanding Ethernet OAM Link Fault Management for ACX Series Routers

The Juniper Networks Junos operating system (Junos OS) for Juniper Networks ACX Series routers allows the Ethernet interfaces on these routers to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities even as Ethernet moves from being solely an enterprise technology to a WAN and access technology, and the standard remains backward compatible with the existing Ethernet technology.

Ethernet OAM provides tools that network management software and network managers can use to determine how a network of Ethernet links is functioning. Ethernet OAM should:

- Rely only on the media access control (MAC) address or virtual LAN identifier for troubleshooting.
- Work independently of the actual Ethernet transport and function over physical Ethernet ports or a virtual service such as a pseudowire.
- Isolate faults over a flat (or single-operator) network architecture or nested or hierarchical (or multiprovider) networks.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/oam-lfm-intro.html#id-understanding-ethernet-oam-link-fault-management-for-acx-series-routers

113. Defendant's ACX Series Universal Metro Routers are configured to verify the functioning of said designated link by analyzing the outcome of said forwarding, each of said physical links being selectable as said designated link, thereby to provide for examination as required for any physical link of said group comprising said single logical link.

You can configure threshold values for fault events that trigger the sending of link event TLVs when the values exceed the threshold. To set threshold values for fault events on an interface, include the **event-thresholds** statement at the **[edit protocols oam ethernet link-fault-management interface]** hierarchy level.

You can also configure OAM threshold values within an action profile and apply the action profile to multiple interfaces. To create an action profile, include the **action-profile** statement at the **[edit protocols oam ethernet link-fault-management]** hierarchy level.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces-ethernet.pdf

Detecting Remote Faults

Fault detection is either based on flags or fault event type, length, and values (TLVs) received in OAM protocol data units (PDUs). Flags that trigger a link fault are:

- Critical Event
- Dying Gasp
- Link Fault

The link event TLVs are sent by the remote DTE by means of event notification PDUs. Link event TLVs are:

- Errored Symbol Period Event
- Errored Frame Event
- Errored Frame Period Event
- Errored Frame Seconds Summary Event

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces-ethernet.pdf

Willful Infringement

114. Defendant has had actual knowledge of the '928 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated May 9, 2017.

115. Defendant has had actual knowledge of the '928 Patent and its infringement thereof at least as of service of Plaintiff's Complaint.

116. Defendant's risk of infringement of the patents-in-suit was either known or was so obvious that it should have been known to Defendant.

117. Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard willfully infringed the '928 Patent. Defendant has thus had actual

notice of the infringement of the '928 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff's valid patent rights, either literally or equivalently.

118. This objective risk was either known or so obvious that it should have been known to Defendant. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

119. Defendant has induced and is knowingly inducing its customers and/or end users to directly infringe the '928 Patent, with the specific intent to encourage such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

120. Defendant has knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the '928 Accused Products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

121. Defendant's indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support that induce its customers and/or end users to directly infringe '928 Patent, including the Juniper Networks ACX Series

Universal Metro Routers Data Sheet and Junos OS Ethernet Interfaces Feature Guide for Routing Devices.

122. Defendant's indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant's indirect infringement further includes providing application notes instructing its customers on infringing uses of the '928 Accused Products. The '928 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the '928 Patent, either literally or equivalently. Defendant knows and intends that customers who purchase the '928 Accused Products will use those products for their intended purpose. For example, Defendant's United States website: https://www.juniper.net, instructs customers to use the '928 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional videos on YouTube (https://www.youtube.com/user/JuniperNetworks/videos), its website, and elsewhere providing instructions on using the '928 Accused Products. Defendant's customers directly infringe the '928 Patent when they follow Defendant's provided instructions on its website, videos, and elsewhere. Defendant's customers who follow Defendant's provided instructions directly infringe claims of the '928 Patent.

123. In addition, Defendant specifically intends that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendant's infringing products. Defendant knows following its

instructions directly infringes claims of the ’928 Patent, including for example Claim 22.

124. Defendant’s customers who follow Defendant’s provided instructions directly infringe the method of claim 22 of the ’928 Patent.

125. Defendant instructs its customers to use its ACX Series Universal Metro Routers (including the ACX500 Router) to implement connectivity fault management (CFM) functions in a network.

Product Description

Juniper Networks® ACX Series Universal Metro Routers are Juniper's response to a shift in metro network architecture, where the access and aggregation layers are extending the operational intelligence from the service provider edge to the access network. The ACX Series simplifies access and aggregation architectures by eliminating unnecessary layers and network overlays, dramatically reducing CapEx and OpEx. Based on architectural simplification and cost reduction, the ACX Series enables service providers and enterprises to adopt the true universal metro paradigm. In addition to Metro Ethernet Forum (MEF) CE2.0 compliance for supporting both Ethernet and IP/MPLS, the ACX Series provides high capacity, scalability, and a secure packet optical transport layer, while delivering industry-leading performance with a wide range of port densities and interface types. Table 1 provides an overview of the interfaces supported on each ACX Series model. Flexibility and upgradability (the ability to mix and match interface types) makes the ACX Series ideal for a wide range of use cases.

https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000397-en.pdf

	Features	ACX500, ACX500-O, ACX500-O-POE	ACX1000, ACX1100	ACX2100, ACX2200	ACX4000	ACX5048, ACX5096
Services	IEEE 802.3 bridge domain	√	√	√	√	√
	PWE (T-LDP)	√	√	√	√	√
	L2VPN (BGP)	√	√	√	√	√
	VPLS (T-LDP/BGP/ LDP autodiscovery)					√
	EVPN-ELINE (PWE)					
	EVPN-ELINE (FXC)					
	Layer 3 VPN	√	√	√	√	√
	Circuit emulation SAToP/CESoPSN/ ATM o MPLS		√[2]	√[2]	√	
	Integrated routing and bridging (IRB)	√	√	√	√	√
	Stateless filters L2-L4	√	√	√	√	√
Class of Service (CoS)	8 queues per port with schedulers and shaping	√	√	√	√	√
	Classification based on 802.1p, DiffServ code point (DSCP), IP-precedence, Exp bit	√	√	√	√	√
	Single-rate policer ingress/egress	√	√	√	√	√
	Two-rate three-color policer ingress/ egress	√	√	√	√	√
	Per-Port Egress Shapping	√	√	√	√	√
	H-QoS					√
OAM and SLA Management	Bidirectional Forwarding Detection (BFD)	√	√	√	√	√
	Connectivity fault management (CFM)	√	√	√	√	√
	Y.1731	√	√	√	√	√[3]
	RFC2544	√	√	√	√	√[4]
	TWAMP	√	√	√	√	

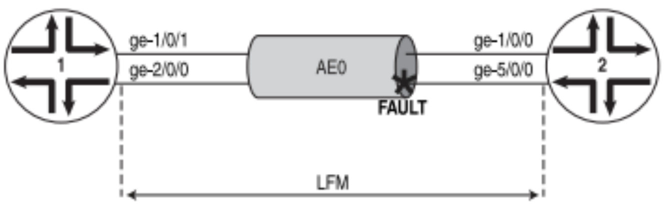
https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000397-en.pdf

126. Defendant instructs its customers to use its ACX Series Universal Metro Routers (including the ACX500 Router) to connect first and second maintenance entities via a link aggregation group (LAG), said LAG comprising a single logical link made up of a plurality of physical links.

In this example, LFM is configured on an aggregated Ethernet interface (AE0) between Router 1 and Router 2. When configured on aggregated Ethernet, LFM runs on all the individual member links. LFM is enabled or disabled on the member links as they are added or deleted from the aggregation group. The status of individual links is used to determine the status of the aggregated interface.

The use of LFM with aggregated Ethernet is shown in Figure 50 on page 688.

Figure 50: Ethernet LFM for Aggregated Ethernet



https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces-ethernet.pdf

127. Defendant instructs its customers to use its ACX Series Universal Metro Routers (including the ACX500 Router) to use said first maintenance entity to select one of said physical links as a designated link for forwarding a CFM message via a designated link of said LAG.

Continuity Check Protocol Parameters Overview

The continuity check protocol is used for fault detection by maintenance end points (MEPs) within a maintenance association. The MEP periodically sends continuity check multicast messages. The continuity check protocol packets use the ethertype value 0x8902 and the multicast destination MAC address 01:80:c2:00:00:32.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces-ethernet.pdf

Understanding Ethernet OAM Link Fault Management for ACX Series Routers

The Juniper Networks Junos operating system (Junos OS) for Juniper Networks ACX Series routers allows the Ethernet interfaces on these routers to support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in access networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. The IEEE 802.3ah standard meets the requirement for OAM capabilities even as Ethernet moves from being solely an enterprise technology to a WAN and access technology, and the standard remains backward compatible with the existing Ethernet technology.

Ethernet OAM provides tools that network management software and network managers can use to determine how a network of Ethernet links is functioning. Ethernet OAM should:

- Rely only on the media access control (MAC) address or virtual LAN identifier for troubleshooting.
- Work independently of the actual Ethernet transport and function over physical Ethernet ports or a virtual service such as a pseudowire.
- Isolate faults over a flat (or single-operator) network architecture or nested or hierarchical (or multiprovider) networks.

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/oam-lfm-intro.html#id-understanding-ethernet-oam-link-fault-management-for-acx-series-routers

128. Defendant instructs its customers to use its ACX Series Universal Metro Routers (including the ACX500 Router) to verify the functioning of said designated link by analyzing the outcome of said forwarding, each of said physical links being selectable as said designated link, thereby to provide for examination as required for any physical link of said group comprising said single logical link.

You can configure threshold values for fault events that trigger the sending of link event TLVs when the values exceed the threshold. To set threshold values for fault events on an interface, include the **event-thresholds** statement at the **[edit protocols oam ethernet link-fault-management interface]** hierarchy level.

You can also configure OAM threshold values within an action profile and apply the action profile to multiple interfaces. To create an action profile, include the **action-profile** statement at the **[edit protocols oam ethernet link-fault-management]** hierarchy level.

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces-ethernet.pdf

Detecting Remote Faults

Fault detection is either based on flags or fault event type, length, and values (TLVs) received in OAM protocol data units (PDUs). Flags that trigger a link fault are:

- Critical Event
- Dying Gasp
- Link Fault

The link event TLVs are sent by the remote DTE by means of event notification PDUs. Link event TLVs are:

- Errored Symbol Period Event
- Errored Frame Event
- Errored Frame Period Event
- Errored Frame Seconds Summary Event

https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/config-guide-network-interfaces/network-interfaces-ethernet.pdf

129. As a result of Defendant's infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement which, by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

COUNT FIVE
INFRINGEMENT OF U.S. PATENT 7,983,150

130. Plaintiff incorporates by reference the allegations in all preceding paragraphs as if fully set forth herein.

131. The '150 Patent, entitled "VPLS FAILURE PROTECTION IN RING NETWORKS" was filed on January 18, 2006 and issued on July 19, 2011.

132. Plaintiff is the assignee and owner of all rights, title and interest to the ’150 Patent, including the right to recover for past infringements, and has the legal right to enforce the patent, sue for infringement, and seek equitable relief and damages.

Technical Description

133. The ’150 Patent addresses technical problems in the prior art of virtual private networks, including that prior art failure protection mechanisms in bi-directional ring networks “do not adequately protect against all failure scenarios that may occur in a VPLS that is provisioned over the ring.” (col. 2, ll. 40–42).

134. The ’150 Patent provides a technical solution to the prior art problems by providing “failure protection mechanisms that can respond to and overcome these sorts of VPLS failure scenarios quickly and efficiently.” (col. 2, ll. 51–53).

135. The ’150 Patent discloses the use of standby connection termination points (CTPs) in a virtual private LAN service. “Each CTP connects the respective node to a network external to the ring network. In the absence of a network failure, these standby CTPs are blocked. When a failure occurs, the nodes in the ring network exchange topology messages and inform one another of the failure. Based on these messages, the nodes may determine that the VPLS has been segmented. In this case, the nodes choose one or more of the standby CTPs to be activated in order to overcome the segmentation.” (col. 2, ll. 56–64).

Direct Infringement

136. Defendant, without authorization or license from Plaintiff, has been and is directly infringing the '150 Patent, either literally or equivalently, as infringement is defined by 35 U.S.C. § 271, including through making, using (including for testing purposes), selling and offering for sale apparatus and methods infringing one or more claims of the '150 Patent. Defendant develops, designs, manufactures, and distributes telecommunications equipment that infringe one or more claims of the '150 Patent. Defendant further provides services that practice methods that infringe one or more claims of the '150 Patent. Defendant is thus liable for direct infringement pursuant to 35 U.S.C. § 271. Exemplary infringing instrumentalities include Juniper EX Series Switches and Juniper QFX Series Switches, and all other substantially similar products (collectively the " '150 Accused Products").

137. Correct Transmission names these exemplary infringing instrumentalities to serve as notice of Defendant's infringing acts, but Correct Transmission reserves the right to name additional infringing products, known to or learned by Correct Transmission or revealed during discovery, and include them in the definition of '150 Accused Products.

138. Defendant is liable for direct infringement pursuant to 35 U.S.C. § 271 for the use, manufacture, sale, offer of sale, importation, or distribution of Defendant's EX Series Switches and QFX Series Switches.

139. Defendant's EX Series Switches and QFX Series Switches are non-limiting examples of switches that operate to meet all limitations of claim 1 of the '150 Patent, either literally or equivalently.

140. Defendant's EX Series Switches and QFX Series Switches are configured to implement a method for communication over a bi-directional ring network that includes nodes connected by spans of the ring network.

> *Ethernet ring protection switching* (ERPS) helps achieve high reliability and network stability. Links in the ring will never form loops that fatally affect the network operation and services availability. The basic idea of an Ethernet ring is to use one specific link to protect the whole ring. This special link is called a *ring protection link (RPL)*. If no failure happens in other links of the ring, the RPL blocks the traffic and is not used. The RPL is controlled by a special node called an *RPL owner*. There is only one RPL owner in a ring. The RPL owner is responsible for blocking traffic over the RPL. Under ring failure conditions, the RPL owner is responsible for unblocking traffic over the RPL. A ring failure results in protection switching of the RPL traffic. An automatic protection switching (APS) protocol is used to coordinate the protection actions over the ring. Protection switching blocks traffic on the failed link and unblocks the traffic on the RPL. When the failure clears, revertive protection switching blocks traffic over the RPL and unblocks traffic on the link on which the failure is cleared.

https://www.juniper.net/documentation/en_US/junos/topics/concept/interfaces-ethernet-ring-protection-switching-overview.html

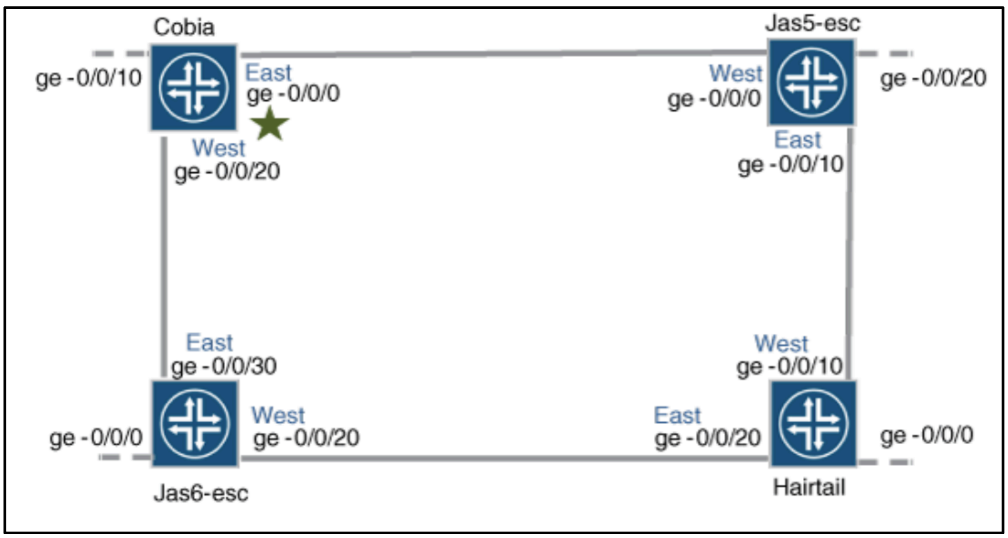
141. Defendant's EX Series Switches and QFX Series Switches are provisioned in a virtual private local area network service (VPLS) to serve users over the bi-directional ring network, the VPLS comprising connection termination points provisioned respectively on a plurality of the nodes so as to connect each of the plurality of the nodes to a second network external to the ring network.

You can configure Ethernet ring protection switching (ERPS) on connected EX Series or QFX Series switches to prevent fatal loops from disrupting a network. (Platform support depends on the Junos OS release in your installation.) ERPS is similar to spanning-tree protocols, but ERPS is more efficient because it is customized for ring topologies. You must configure at least three switches to form a ring.

https://www.juniper.net/documentation/en_US/junos/topics/example/interfaces-ethernet-ring-protection-switching-ex-series.html#

This example creates one protection ring (called a node ring) named erp1 on four switches connected in a ring by trunk ports as shown in Figure 1. Because the links are trunk ports, the VLAN named erp-control-vlan-1 is used for erp1 traffic. The east interface of each switch is connected with the west interface of an adjacent switch. Cobia is the RPL owner, with interface ge-0/0/0 configured as an RPL end interface. The interface ge-0/0/0 of Jas5-esc is configured as the RPL neighbor interface. In the idle state, the RPL end blocks the control VLAN and data channel VLAN for this particular ERP instance—the blocked port on Cobia is marked with a star in Figure 1.

https://www.juniper.net/documentation/en_US/junos/topics/example/interfaces-ethernet-ring-protection-switching-ex-series.html#



https://www.juniper.net/documentation/en_US/junos/topics/example/interfaces-ethernet-ring-protection-switching-ex-series.html#

142. Defendant's EX Series Switches and QFX Series Switches activate a selected connection termination point, to establish a connection between the bi-directional ring network and the second network.

5. In addition, configure either the east interface or the west interface (but not both) as a link end. For example, configure the east interface:

```
[edit protocols protection-group ethernet-ring ring-name]
user@switch# set east-interface ring-protection-link-end
```

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/ethernet-ring-protection-cli.html

143. Defendant's EX Series Switches and QFX Series Switches are configured so that as long as the nodes and spans are fully operational, all of the connection termination points except the selected connection termination point are maintained in a deactivated state, so that only the selected connection termination point to the second network is active.

You can configure Ethernet ring protection switching (ERPS) on connected switches to prevent fatal loops from disrupting a network. ERPS is similar to spanning-tree protocols, but ERPS is more efficient than spanning-tree protocols because it is customized for ring topologies. You must configure at least three switches to form a ring. One of the links, called the ring protection link (RPL) end interface, is blocked until another link fails—at this time the RPL link is unblocked, ensuring connectivity.

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/ethernet-ring-protection-cli.html

Under normal operating conditions, when Ethernet ring protection is configured correctly, the ring protection link (RPL) owner (Router 1 in the configuration example) will see the following:

Router 1 Operational Commands (Normal Ring Operation)

`user@router1> show protection-group ethernet-ring aps`

```
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg101               NR             No        Yes

Originator  Remote Node ID
Yes
```

Note that the ring protection link is blocked and the node is marked as the originator of the protection.

`user@router1> show protection-group ethernet-ring interface`

```
Ethernet ring port parameters for protection group pg101

Interface     Control Channel  Forward State  Ring Protection Link End
ge-1/0/1      ge-1/0/1.1       discarding     Yes
ge-1/2/4      ge-1/2/4.1       forwarding     No

Signal Failure  Admin State
Clear           IFF ready
Clear           IFF ready
```

https://www.juniper.net/documentation/en_US/junos/topics/task/operational/layer-2-ethernet-oam-ring-protection-viewing-example-normal-conditions-mx-solutions.html

144. Defendant's EX Series Switches and QFX Series Switches are configured to exchange messages among the nodes indicative of a failure in at least two spans of the ring network causing a segmentation of the ring network and leading to an isolation of a first node of the ring network from at least one second node of the ring network.

This section assumes that Ethernet ring protection is configuring correctly, that Router 1 is the ring protection link (RPL) owner, and that there is a link failure between Router 2 and Router 3 in the configuration example.

Router 1 Operational Commands (Ring Failure Condition)

```
user@router1> show protection-group ethernet-ring aps
```

```
Ethernet Ring Name   Request/state   No Flush   Ring Protection Link Blocked
pg101                SF              NO         No

Originator   Remote Node ID
No           00:01:02:00:00:01
```

https://www.juniper.net/documentation/en_US/junos/topics/task/operational/layer-2-ethernet-oam-ring-protection-viewing-example-failure-conditions-mx-solutions.html

145. Defendant's EX Series Switches and QFX Series Switches are configured to, responsively to the messages, activate at least one of the deactivated connection termination points so as to overcome the segmentation and maintain connectivity of the first node with the at least one second node of the ring network, without creating a loop in the VPLS via the second network.

Note that the ring protection link is no longer blocked and the node is no longer marked as originator.

```
user@router1> show protection-group ethernet-ring interface

Ethernet ring port parameters for protection group pg101

Interface     Control Channel  Forward State  Ring Protection Link End
ge-1/0/1      ge-1/0/1.1       forwarding     Yes
ge-1/2/4      ge-1/2/4.1       forwarding     No

Signal Failure  Admin State
Clear           IFF ready
Clear           IFF ready
```

https://www.juniper.net/documentation/en_US/junos/topics/task/operational/layer-2-ethernet-oam-ring-protection-viewing-example-failure-conditions-mx-solutions.html

Willful Infringement

146. Defendant has had actual knowledge of the ’150 Patent and its infringement thereof at least as of receipt of Plaintiff's notice letter dated May 9, 2017.

147. Defendant has had actual knowledge of the ’150 Patent and its infringement thereof at least as of service of Plaintiff's Complaint.

148. Defendant's risk of infringement of the patents-in-suit was either known or was so obvious that it should have been known to Defendant.

149. Notwithstanding this knowledge, Defendant has knowingly or with reckless disregard willfully infringed the ’150 Patent. Defendant has thus had actual notice of the infringement of the ’150 Patent and acted despite an objectively high likelihood that its actions constituted infringement of Plaintiff's valid patent rights, either literally or equivalently.

150. This objective risk was either known or so obvious that it should have been known to Defendant. Accordingly, Plaintiff seeks enhanced damages pursuant to 35 U.S.C. §§ 284 and 285.

Indirect Infringement

151. Defendant has induced and is knowingly inducing its customers and/or end users to directly infringe the ’150 Patent, with the specific intent to encourage such infringement, and knowing that the induced acts constitute patent infringement, either literally or equivalently.

152. Defendant has knowingly contributed to direct infringement by its customers by having imported, sold, and/or offered for sale, and knowingly importing, selling, and/or offering to sell within the United States the accused products which are not suitable for substantial non-infringing use and which are especially made or especially adapted for use by its customers in an infringement of the asserted patent.

153. Defendant’s indirect infringement includes, for example, providing data sheets, technical guides, demonstrations, software and hardware specifications, installation guides, and other forms of support, that induce its customers and/or end users to directly infringe ’150 Patent. Defendant’s indirect infringement additionally includes marketing its products for import by its customers into the United States. Defendant’s indirect infringement further includes providing application notes instructing its customers on infringing uses of the ’150 Accused Products. The ’150 Accused Products are designed in such a way that when they are used for their intended purpose, the user infringes the ’150 Patent, either literally or equivalently.

Defendant knows and intends that customers who purchase the ’150 Accused Products will use those products for their intended purpose. For example, Defendant’s United States website https://www.juniper.net, instructs customers to use the ’150 Accused Products in numerous infringing applications. Furthermore, Defendant provides instructional videos on YouTube (https://www.youtube.com/user/ JuniperNetworks/ videos), its website, and elsewhere providing instructions on using the ’150 Accused Products. Defendant’s customers directly infringe the ’150 Patent when they follow Defendant’s provided instructions on its website, videos, and elsewhere. Defendant’s customers who follow Defendant’s provided instructions directly infringe claims of the ’150 Patent.

154. In addition, Defendant specifically intends that its customers, such as United States distributors, retailers and consumer product companies, will import, use, and sell infringing products in the United States to serve and develop the United States market for Defendant’s infringing products. Defendant knows following its instructions directly infringes claims of the ’150 Patent, including claim 1.

155. Defendant’s customers who follow Defendant’s provided instructions directly infringe the method of claim 1 of the ’150 Patent.

156. Defendant instructs its customers to use its EX Series Switches and QFX Series Switches in a method for communication over a bi-directional ring network that includes nodes connected by spans of the ring network.

> *Ethernet ring protection switching* (ERPS) helps achieve high reliability and network stability. Links in the ring will never form loops that fatally affect the network operation and services availability. The basic idea of an Ethernet ring is to use one specific link to protect the whole ring. This special link is called a *ring protection link (RPL)*. If no failure happens in other links of the ring, the RPL blocks the traffic and is not used. The RPL is controlled by a special node called an *RPL owner*. There is only one RPL owner in a ring. The RPL owner is responsible for blocking traffic over the RPL. Under ring failure conditions, the RPL owner is responsible for unblocking traffic over the RPL. A ring failure results in protection switching of the RPL traffic. An automatic protection switching (APS) protocol is used to coordinate the protection actions over the ring. Protection switching blocks traffic on the failed link and unblocks the traffic on the RPL. When the failure clears, revertive protection switching blocks traffic over the RPL and unblocks traffic on the link on which the failure is cleared.

https://www.juniper.net/documentation/en_US/junos/topics/concept/interfaces-ethernet-ring-protection-switching-overview.html

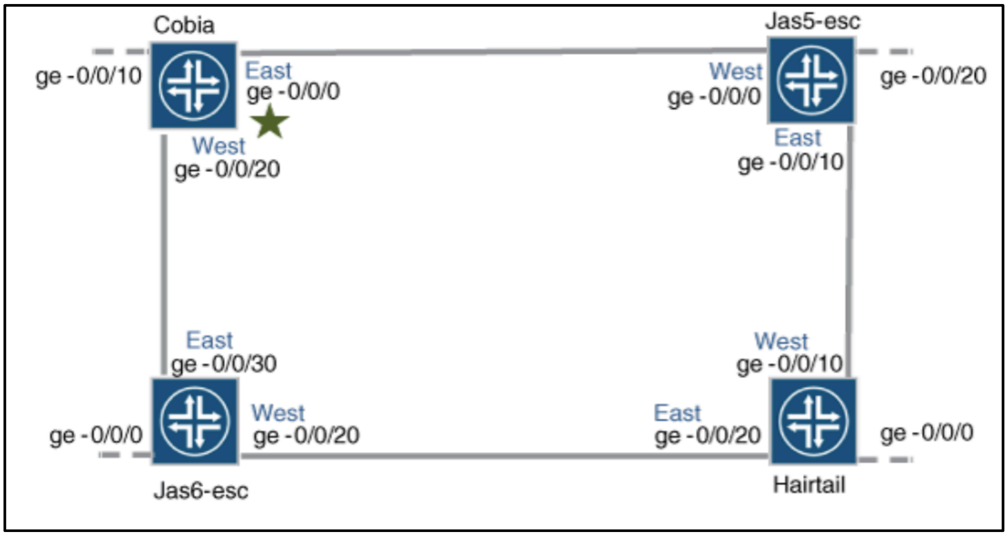
157. Defendant instructs its customers to use its EX Series Switches and QFX Series Switches to provision a virtual private local area network service (VPLS) to serve users over the bi-directional ring network, the VPLS comprising connection termination points provisioned respectively on a plurality of the nodes so as to connect each of the plurality of the nodes to a second network external to the ring network.

> You can configure Ethernet ring protection switching (ERPS) on connected EX Series or QFX Series switches to prevent fatal loops from disrupting a network. (Platform support depends on the Junos OS release in your installation.) ERPS is similar to spanning-tree protocols, but ERPS is more efficient because it is customized for ring topologies. You must configure at least three switches to form a ring.

https://www.juniper.net/documentation/en_US/junos/topics/example/interfaces-ethernet-ring-protection-switching-ex-series.html#

This example creates one protection ring (called a node ring) named erp1 on four switches connected in a ring by trunk ports as shown in Figure 1. Because the links are trunk ports, the VLAN named erp-control-vlan-1 is used for erp1 traffic. The east interface of each switch is connected with the west interface of an adjacent switch. Cobia is the RPL owner, with interface ge-0/0/0 configured as an RPL end interface. The interface ge-0/0/0 of Jas5-esc is configured as the RPL neighbor interface. In the idle state, the RPL end blocks the control VLAN and data channel VLAN for this particular ERP instance—the blocked port on Cobia is marked with a star in Figure 1.

https://www.juniper.net/documentation/en_US/junos/topics/example/interfaces-ethernet-ring-protection-switching-ex-series.html#



https://www.juniper.net/documentation/en_US/junos/topics/example/interfaces-ethernet-ring-protection-switching-ex-series.html#

158. Defendant instructs its customers to use its EX Series Switches and QFX Series Switches to activate a selected connection termination point, to establish a connection between the bi-directional ring network and the second network.

5. In addition, configure either the east interface or the west interface (but not both) as a link end. For example, configure the east interface:

```
[edit protocols protection-group ethernet-ring ring-name]
user@switch# set east-interface ring-protection-link-end
```

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/ethernet-ring-protection-cli.html

159. Defendant instructs its customers to use its EX Series Switches and QFX Series Switches, as long as the nodes and spans are fully operational, to maintain all of the connection termination points except the selected connection termination point in a deactivated state, so that only the selected connection termination point to the second network is active.

You can configure Ethernet ring protection switching (ERPS) on connected switches to prevent fatal loops from disrupting a network. ERPS is similar to spanning-tree protocols, but ERPS is more efficient than spanning-tree protocols because it is customized for ring topologies. You must configure at least three switches to form a ring. One of the links, called the ring protection link (RPL) end interface, is blocked until another link fails—at this time the RPL link is unblocked, ensuring connectivity.

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/ethernet-ring-protection-cli.html

Under normal operating conditions, when Ethernet ring protection is configured correctly, the ring protection link (RPL) owner (Router 1 in the configuration example) will see the following:

Router 1 Operational Commands (Normal Ring Operation)

```
user@router1> show protection-group ethernet-ring aps
```

```
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg101               NR             No        Yes

Originator  Remote Node ID
Yes
```

Note that the ring protection link is blocked and the node is marked as the originator of the protection.

```
user@router1> show protection-group ethernet-ring interface
```

```
Ethernet ring port parameters for protection group pg101

Interface     Control Channel  Forward State  Ring Protection Link End
ge-1/0/1      ge-1/0/1.1       discarding     Yes
ge-1/2/4      ge-1/2/4.1       forwarding     No

Signal Failure  Admin State
Clear           IFF ready
Clear           IFF ready
```

https://www.juniper.net/documentation/en_US/junos/topics/task/operational/layer-2-ethernet-oam-ring-protection-viewing-example-normal-conditions-mx-solutions.html

160. Defendant instructs its customers to use its EX Series Switches and QFX Series Switches to exchange messages among the nodes indicative of a failure in at least two spans of the ring network causing a segmentation of the ring network and leading to an isolation of a first node of the ring network from at least one second node of the ring network.

This section assumes that Ethernet ring protection is configuring correctly, that Router 1 is the ring protection link (RPL) owner, and that there is a link failure between Router 2 and Router 3 in the configuration example.

Router 1 Operational Commands (Ring Failure Condition)

```
user@router1> show protection-group ethernet-ring aps
```

```
Ethernet Ring Name   Request/state   No Flush   Ring Protection Link Blocked
pg101                SF              NO         No

Originator   Remote Node ID
No           00:01:02:00:00:01
```

https://www.juniper.net/documentation/en_US/junos/topics/task/operational/layer-2-ethernet-oam-ring-protection-viewing-example-failure-conditions-mx-solutions.html

161. Defendant instructs its customers to use its EX Series Switches and QFX Series Switches, responsively to the messages, to activate at least one of the deactivated connection termination points so as to overcome the segmentation and maintain connectivity of the first node with the at least one second node of the ring network, without creating a loop in the VPLS via the second network.

Note that the ring protection link is no longer blocked and the node is no longer marked as originator.

```
user@router1> show protection-group ethernet-ring interface
```

```
Ethernet ring port parameters for protection group pg101

Interface     Control Channel   Forward State   Ring Protection Link End
ge-1/0/1      ge-1/0/1.1        forwarding      Yes
ge-1/2/4      ge-1/2/4.1        forwarding      No

Signal Failure   Admin State
Clear            IFF ready
Clear            IFF ready
```

https://www.juniper.net/documentation/en_US/junos/topics/task/operational/layer-2-ethernet-oam-ring-protection-viewing-example-failure-conditions-mx-solutions.html

162. As a result of Defendant's infringement, Plaintiff has suffered monetary damages, and is entitled to an award of damages adequate to compensate it for such infringement, which by law, can be no less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 US.C. § 284.

V. NOTICE

163. Correct Transmission has complied with the notice requirement of 35 U.S.C. § 287 and does not currently distribute, sell, offer for sale, or make products embodying the Asserted Patents. This notice requirement has been complied with by all relevant persons at all relevant times.

VI. JURY DEMAND

164. Plaintiff demands a trial by jury of all matters to which it is entitled to trial by jury, pursuant to FED. R. CIV. P. 38.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment and seeks relief against Defendant as follows:

A. That the Court determine that one or more claims of the Asserted Patents is infringed by Defendant, both literally and under the doctrine of equivalents;

B. That the Court determine that one or more claims of the Asserted Patents is indirectly infringed by Defendant;

C. That the Court award damages adequate to compensate Plaintiff for the patent infringement that has occurred, together with prejudgment and post-judgment interest and costs, and an ongoing royalty for continued infringement;

D. That the Court permanently enjoin Defendant pursuant to 35 U.S.C. § 283;

E. That the Court find this case to be exception pursuant to 35 U.S.C. § 285;

F. That the Court determine that Defendant's infringements were willful;

G. That the Court award enhanced damages against Defendant pursuant to 35 U.S.C. § 284;

H. That the Court award reasonable attorneys' fees; and

I. That the Court award such other relief to Plaintiff as the Court deems just and proper.

Dated: July 23, 2020

Respectfully Submitted,

/s/ E. Leon Carter

E. Leon Carter
lcarter@carterarnett.com
Texas Bar No. 03914300
Scott W. Breedlove
sbreedlove@carterarnett.com
State Bar No. 00790361
Joshua J. Bennett
jbennett@carterarnett.com
Texas Bar No. 24059444
Minghui Yang
myang@carterarnett.com
Texas Bar No. 24091486
CARTER ARNETT PLLC
8150 N. Central Expy, 5th Floor
Dallas, Texas 75206
Telephone No. (214) 550-8188
Facsimile No. (214) 550-8185

Bradley D. Liddle
(*application for admission pending*)
bliddle@carterarnett.com
Texas Bar No. 24074599
Monica Litle
(*application for admission pending*)
mlitle@carterarnett.com
Texas Bar No. 24102101
CARTER ARNETT PLLC
8150 N. Central Expy, 5th Floor
Dallas, Texas 75206
Telephone No. (214) 550-8188
Facsimile No. (214) 550-8185

ATTORNEYS FOR PLAINTIFF